나무위키

Hyphanet

최근 수정 시각: 2026-08-23 07:13:15

분류:소프트웨어 | 프록시 | 다크 웹

목차

1. 개요
2. Hyphanet의 이해
   2.1. 좁은 세상의 네트워크
   2.2. 데이터 저장소
   2.3. Hyphanet의 경로
3. Hyphanet의 특징
   3.1. Opennet 모드와 Darknet 모드
4. Hyphanet(Opennet 모드) 사용법
   4.1. 익명성 유지를 위한 원칙
   4.2. 토어 브라우저 세팅법
   4.3. 파일을 공유하는 법
   4.4. FMS(Freenet Message System) 사용법
   4.5. Frost-Next 사용법
   4.6. Hyphanet 클라이언트 설정법
      4.6.1. wrapper 폴더 안의 "wrapper.conf" 파일 설정
      4.6.2. Hyphanet 폴더 안의 "freenet.ini" 파일 설정
      4.6.3. Hyphanet 본체 설정
      4.6.4. Frost 설정
   4.7. Hyphanet 삭제법
5. Hyphanet(Darknet 모드) 사용법
   5.1. 설정하기
   5.2. 친구와 서로 연결하기
   5.3. 메시지(N2NTM) 보내기
   5.4. 파일 공유하기
6. Hyphanet을 권장하지 않는 이유
7. Freenet over I2P
8. 억압적인 국가에서의 검열 우회
9. 같이 보기

Hyphanet 홈페이지
Frost 홈페이지

1. 개요

2023년 6월 26일부터 프리넷(Freenet)에서 하이퍼넷(Hyphanet)으로 명칭이 변경되었다. Hyphanet 홈페이지의 설명

Hyphanet의 핵심은 게시자가 더 이상 온라인 상태가 아닐 때에도 다른 사람이 게시한 콘텐츠에 접근할 수 있다는 것이다. Tor나 I2P는 콘텐츠에 접근하려면 온라인 상태인 서버가 반드시 필요하며 만약 서버가 폐쇄되면 콘텐츠에 접근할 수 없게 된다. 반면 Hyphanet은 폐쇄할 서버라는 게 없으며 게시자가 오프라인인 상태에서도 콘텐츠 배포가 가능하다.
또한 Hyphanet은 검열 저항성(콘텐츠가 삭제되지 않고 계속 살아남음)이 뛰어나다. Tor나 I2P와 달리 서버를 폐쇄하는 방식으로 콘텐츠를 제거하는 것이 불가능하며 게시한 본인조차 한번 업로드한 콘텐츠는 삭제가 불가능하다. Hyphanet 상에서 콘텐츠가 삭제되는 유일한 방법은 그 콘텐츠가 인기가 없어서 아무도 찾지 않았을 때 뿐이다. 인기가 없는 파일은 어느 순간 Hyphanet 상에서 삭제된다.

익명성(신원을 식별할 수 없음)은 Hyphanet의 핵심이 아니다. 그렇다고 익명성이 아예 없는 것은 아니지만 Opennet 모드 Hyphanet의 익명성은 Tor/I2P보다 약하다. Hyphanet은 그럴듯한 부인가능성(Plausible Deniability)과 제한된 수준(사법기관의 어그로를 심하게 끌지 않는 수준)에서의 익명성을 제공한다. 그럴듯한 부인가능성(Plausible Deniability)이란 '네 말이 맞을 가능성도 있지만, 그렇지 않을 가능성도 있다'는 식으로 공격자로 하여금 우리에게 불리한 어떤 가설을 확실하게 증명하지 못하게 만드는 것을 말한다.#[1]

Hyphanet 상의 저장공간은 무한하지 않고 이미 기존의 콘텐츠로 가득 채워져 있다. Hyphanet에 새 콘텐츠를 삽입하면 기존에 있던 콘텐츠가 Hyphanet 네트워크 상에서 삭제된다. 따라서 Hyphanet 상에 대용량 파일을 올리면 얼마 못 가 파일의 일부분이 삭제되면서 파일이 망가질 가능성이 높다. 그러므로 대용량 파일 공유에 Hyphanet을 사용하는 것은 권장하지 않는다.

Hyphanet은 사용자의 회선에 따른 통신 속도, 사용자가 결정한 수준의 익명성에 맞게 설정을 한다. Hyphanet 본체는 브라우저 형태이지만, 많은 사용자들은 Hyphanet 본체를 기존에 익숙한 P2P 형태로 보여주는 Frost를 많이 사용한다. 사용자들은 Hyphanet 본체를 통한 Frost에서 채팅을 할 수도, 자료에 대한 Key(일종의 주소)를 주고받기도 한다.

Frost에는 public board와 secure board라는 두 가지 종류의 게시판이 있다. public board는 특정 게시판의 이름의 board를 추가하면 안의 내용을 볼 수 있지만, secure board는 사용자가 특정 게시판의 이름뿐만 아니라 Private key와 Public key 이 둘을 기입해야 안의 내용을 볼 수 있다.

일본에서는 기존 P2P들이 단속에 속수무책으로 뚫리자 Hyphanet이 각광을 받으며 한때 2ch download에서 Hyphanet 관련 스레드가 올라왔다. 현재는 불법으로 미연시, 에로게 립을 공유하는 Justice 씨가 활동하는 장소로 인식되고 있다.

만약 Hyphanet에서 일본어 포럼(FMS, Frost)을 찾는다면 다음 글을 참고할 수 있다. 5ch를 이용하는 유저들이 많아 보인다. 일본 커뮤니티를 구경할 때는 혐한 성향을 어느 정도 감안하고 봐야 하는데 Hyphanet의 일본어 포럼 또한 예외는 아니다. 일본 Hyphanet 탐방 후기

황금방패때문인지 중국어 포럼은 죽은 것으로 보인다.

Hyphanet에서 한국어 포럼(FMS, Frost)을 찾아서 볼 수 있다.
한국 Hyphanet Frost 포럼
한국 Hyphanet FMS 포럼

구글에서 Hyphanet 웹사이트를 검색하려면 'AQACAAE'를 검색하면 된다. 앞에 'USK'가 붙어있는 것이 사이트의 주소이다. 관련 링크, 예시

Hyphanet FAQ를 참고하면 좋다.#

Hyphanet Quick Start 가이드에 Hyphanet에 대한 자세한 정보가 많으니 참고한다. 한국어, 영어

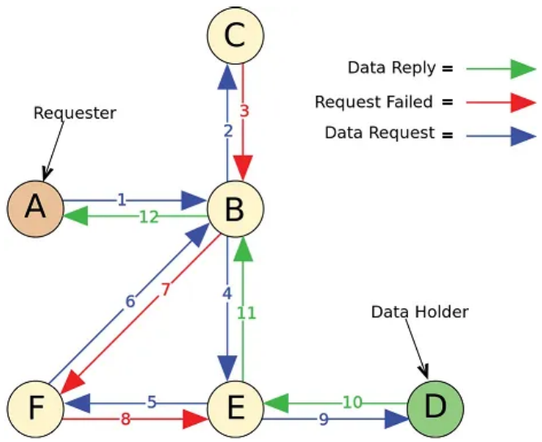
어느 러시아인이 쓴 Hyphanet FAQ 글 또한 참고한다.# @

2. Hyphanet의 이해

Hyphanet은 일종의 '분산 암호화 데이터 저장소'로 볼 수 있다. Hyphanet에 파일을 삽입하면 파일이 여러 조각으로 쪼개진 채 암호화(분산+암호화)돼서 내가 아닌 다른 사람들의 HDD/SSD에 저장된다. 비유적으로 표현하자면 '피자 한 판.jpg'를 여러 조각으로 나눠서 암호화한 뒤 다른 사람들에게 나눠준다고 생각하면 된다. 파일을 불러오려면 다시 말해 피자 조각들을 모아 피자 한 판으로 만들려면 키(Key)가 필요하다.

Node라는 말 대신 남의 컴퓨터, 남의 저장장치, 남의 HDD, 남의 SSD라고 생각하면 더 직관적이고 이해하기 쉬울 것이다.

Hyphanet에서 파일을 불러오는 방식은 입소문이나 바이럴 마케팅 같은 것들을 생각하면 된다.



A가 "이러한 키(Key)에 해당하는 파일을 가진 사람을 찾습니다" 하고 주변 사람들에게 외치면 주변 사람들도 다시 자기 주변 사람들에게 외치고 이를 반복하다 보면 파일 조각을 가지고 있는 D를 찾게 되는 것이다.

만약 파일이 인기가 없어서 아무도 찾지 않거나 피자 조각을 가지고 있던 컴퓨터들이 리셋이나 파손 등으로 망가지는 등 피자의 일부 조각이 Hyphanet 상에서 사라진다면 파일을 요청해도 피자 한 판을 완성할 수 없게 된다. 이때 파일을 다시 살리기 위해 하는 행위를 힐링(Healing)이라고 한다. 이를 사람이 매번 수동으로 하면 귀찮으니까 플러그인으로 만든 게 KeepAlive라는 플러그인이다.

크기가 작은 파일은 8조각으로 나눠지지만 대용량 파일은 더 많은 조각으로 나눠지게 된다. 예를 들어 대용량 피자 하나가 100조각이라고 가정한다면 크기가 작은 피자는 8조각만 살아있으면 되지만 대용량 피자는 100조각이 모두 살아있어야 한다. 99조각이 살아있어도 1조각이 없으면 대용량 피자 한 판이 만들어질 수 없고 이는 파일이 망가졌다 또는 파일이 깨졌다고 볼 수 있다. 물론 KeepAlive 플러그인을 쓴다지만 대용량 파일의 수명이 크기가 작은 파일에 비해 짧은 것은 변함 없다.

Hyphanet은 하나의 큰 저장 장치로 생각될 수 있다. 사용자가 Hyphanet에 파일을 저장할 때, 사용자는 그 파일을 검색하는 데 사용되는 일종의 키(key)를 받는다. 사용자가 키(key)를 Hyphanet에 입력할 때, 해당 파일이 있다면 Hyphanet은 적절한 파일로 불러올 수 있다. 저장 공간은 Hyphanet에 연결되어 있는 모두에게서 분배된다.

Hyphanet은 분산화되고 익명화된 P2P(peer-to-peer) 네트워크이다. 이 사용자가 연결하는 노드들은 가장 가까운 이웃들만 알 수 있으며, 전체 네트워크 구조가 어떻게 조직되었는지는 알 수가 없다.

좀 더 쉽게 설명하자면, 어떠한 문서(파일, 페이지 등)에 대한 정보가 필요하여 자신의 근접한 노드에 해당 정보를 보내면[2] 그 파일과 같거나 유사한 파일의 정보가 찾아질 때까지 그 노드 또한 근접한 노드에 요청을 발송한다. 점차 그 요청이 곳곳에 퍼지게 되지만 누가 이 요청을 보냈는지는 멀어질수록 특정하기는 힘들어진다. 단순히 한 사람이 한 사람에게 요청을 보냈다는 기록만 많기 때문.
요청이 해당 문서를 가진 노드에 도착하고, 그 문서를 가진 노드는 해당 문서를 자신에게 요청을 보낸 노드에 암호화시켜 송신한다. 이때 그 받은 마지막 요청자에게 보내고, 그 마지막 요청자는 해당 문서를 복사하여 소지하며 자신에게 요청한 사람에게 또 보낸다. 이를 반복하면 결국 최초 요청자에게 파일이 도착하게 된다.[비유]

Hyphanet에서는 누가 파일을 삽입했는지, 누가 해당 파일을 요청했는지, 파일이 어디에 저장되었는지 아무도 모른다. 따라서 검열하기가 매우 어렵다.

2.1. 좁은 세상의 네트워크

Hyphanet은 좁은 세상의 네트워크들을 바탕으로 만들어졌다. 사용자가 이미 알고 있는 사람들의 노드들을 연결함으로써, 사용자가 아는 사람들은 차례로 그들이 아는 사람들을 연결하고, 누군가는 프리넷 네트워크에 있는 모든 노드들에 도달할 수 있다.

2.2. 데이터 저장소

모든 Hyphanet 노드들은 파일을 저장하기 위해 사용자들의 하드 드라이브 공간의 일부를 사용한다. 파일들은 Hyphanet 설치 디렉터리의 저장 디렉터리에 암호화된 채 저장된다.

다른 P2P 네트워크와 다르게, 사용자는 데이터 저장소에 저장된 것에 아무런 영향을 줄 수가 없다. 대신에, 파일들은 그들이 얼마나 인기 있는가에 따라 유지되거나 삭제된다. 이는 프리넷이 검열을 피할 수 있음을 보장하는 것이다. Hyphanet에서 어떤 것을 삭제할 수 있는 유일한 방법은 그것을 검색하지 않는 것이며, 모든 사람들은 이를 희망한다.

사용자의 지역적인 Hyphanet 데이터 저장소에 저장한 파일을 알아내는 것은 어렵지만도, 불가능이지는 않다. 이는 사용자의 하드 드라이브의 데이터 저장소에 있는 어떤 종류의 물건들에 관해서 알고 있어도 모른 척을 할 수 있게 만든다.

Hyphanet은 얼마나 공간을 사용할 수 있는가에 따라 초기 크기를 정하고 사용자가 언제든지 저장하는 크기를 바꿀 수 있다. 램(RAM)보다 더 큰 저장 공간을 사용하지만, 사용자에게 나은 검색을 제공하고 Hyphanet 전체에 도움을 준다.

2.3. Hyphanet의 경로

초기에, 각 노드는 그것을 알고 있는 또 다른 노드들의 실행에 대한 아무런 정보를 가지지 않는다. 이는 요청의 경로는 반드시 무작위라는 것을 의미한다. 그러나 서로 다른 노드들은 서로 다른 무작위성을 가지기 때문에, 그들은 주어진 키(key), 즉 요청을 보낼 곳이 일치하지 않는다. 그래서 Hyphanet에 새롭게 들어온 데이터는 다소 무작위 하게 분배된다.

더 많은 문서들은 같은 노드에 의해서 삽입되고, 그들은 데이터 항목들의 비슷한 키(key)로 모이기 시작한다. 같은 경로의 규칙들은 그들 전부에 사용되기 때문이다. 더 중요한 것으로, 서로 다른 노드들로부터의 데이터 항목들과 요청들은 "엇갈린 경로들"로써, 그들 역시 모인 정보를 공유하기 시작한다.

결과적으로, 노드들이 키 공간(key space)에서 가까운 데이터 항목들을 수용하는 경향이 있고, 이 네트워크는 분배되고 모여진 체계들을 자체적으로 조직한다. 아마도 네트워크를 통틀어 이런 클러스터들, 여러 번 복제되어서 주어진 어떠한 문서, 얼마나 그것을 사용했는가에 따라 복합적이다.

3. Hyphanet의 특징

- 노드 자체에 파일 정보가 포함되지 않는다.
- 파일은 전부 암호화된 중계 노드를 통해서 전송을 한다.

이 2가지 특징에서 누가, 어떤 파일을 가지고 있는지를 전혀 모른다. 이로써 그럴듯한 부인가능성(Plausible Deniability)과 제한된 수준(사법기관의 어그로를 심하게 끌지 않는 수준)에서의 익명성을 확보하게 된다. 그렇다고 트래픽 해석이나 소프트웨어 오류, 설정 오류, 동시에 Hyphanet 자체가 불법으로 할 수 있고, 절대로 특정되지 않는다는 것은 아니다. 아직까지는 체포된 사람은 세계에서 한 명도 나오지 않았다.

어디까지나 Hyphanet의 목적은 저작권 침해가 아니라 특정의 사상과 권력에 지배되지 않는 자유로운 발언, 표현의 장을 제공하는 데에 있다.

3.1. Opennet 모드와 Darknet 모드

Hyphanet에 연결하는 방법은 임의의 낯선 사람과 자동으로 연결되는 Opennet 모드와 신뢰할 수 있는 사람에게만 연결되는 Darknet 모드 두 가지가 있다. Darknet 모드는 신뢰할 수 있는 사람들과만 연결되기 때문에 Opennet 모드보다 더 안전하다. 그러나 Hyphanet을 쓰는 대다수의 사람들은 신뢰할 수 있는 사람을 찾는 것이 어렵기 때문에 Opennet 모드를 사용한다.

Hyphanet은 Tor나 I2P와 달리 IP를 숨기지 않는다는 점을 고려하면, 낯선 사람들과 연결되는 Opennet 모드의 경우 신뢰할 수 있는 VPN을 Hyphanet과 함께 사용하여 '유저 -> VPN -> Hyphanet -> 인터넷'으로 연결하는 것이 더 좋을 수도 있다. 참고로 '유저 -> Tor -> Hyphanet -> 인터넷'은 불가능하다.🔗관련 글

Hyphanet에 대해 검색해 보고 알아볼수록 Opennet이 처음 생각했던 것보다 안전하지 않다는 것을 알게 될 것이다. Hyphanet에서 사법기관의 어그로를 심하게 끄는 극히 위험한 콘텐츠를 공유하는 사람들에 대해서, 도덕적인 측면과 동시에 **기술적인 측면**에서 이해 못하게 될 수도 있다.

4. Hyphanet(Opennet 모드) 사용법

4.1. 익명성 유지를 위한 원칙

- PeerGuardian이나 PeerBlock을 사용하고 신뢰할 수 없는 IP 주소의 접속을 막는다.
- 클립보드에 복사한 정보는 정기적으로 지운다.
- Hyphanet 웹 사이트를 열람하는 경우에 쿠키, 사용 이력을 남기지 않는다.

(Hyphanet에서만 접속 가능한 사이트인 freesite에서 외부로의 접속은 Hyphanet proxy에 의해서 모두 걸러진다.)

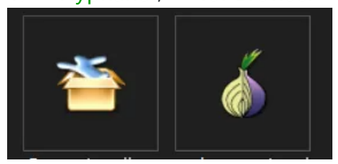
4.2. 토어 브라우저 세팅법

이 문단에서는 Tor Browser를 사용하여 Hyphanet에 접속하는 법을 서술한다.
주의사항
1. 아래의 글은 토어 브라우저를 쓸 뿐 토어 네트워크는 쓰지 않는다.
2. 애초에 Windows는 프라이버시에 아주 나쁜 OS이다. 리눅스에서 Hyphanet을 이용하는 것을 매우 권장한다.
3. Virtualbox 같은 가상머신을 이용하면 매우 좋다. 혹시라도 탐방하다가 악성코드에 감염되더라도 가상머신이 막아줄 수 있기 때문이다.
4. Whonix나 Qubes OS에서 Hyphanet을 사용하는 것이 가장 안전하다. 참고로 Tails OS는 Hyphanet 사용이 불가능하다.
5. 익명 네트워크 특성상 탐방하다가 불법 사이트를 발견할 수도 있는데 들어가지 않는 것을 적극 권장한다.
6. 위 가이드의 작성자는 Hyphanet에 대한 이해가 매우 빈약하다. 그러므로 만약 다른 사람의 글과 위 가이드의 내용이 충돌한다면 위 가이드가 틀린 내용이라고 여기는 것이 좋다.

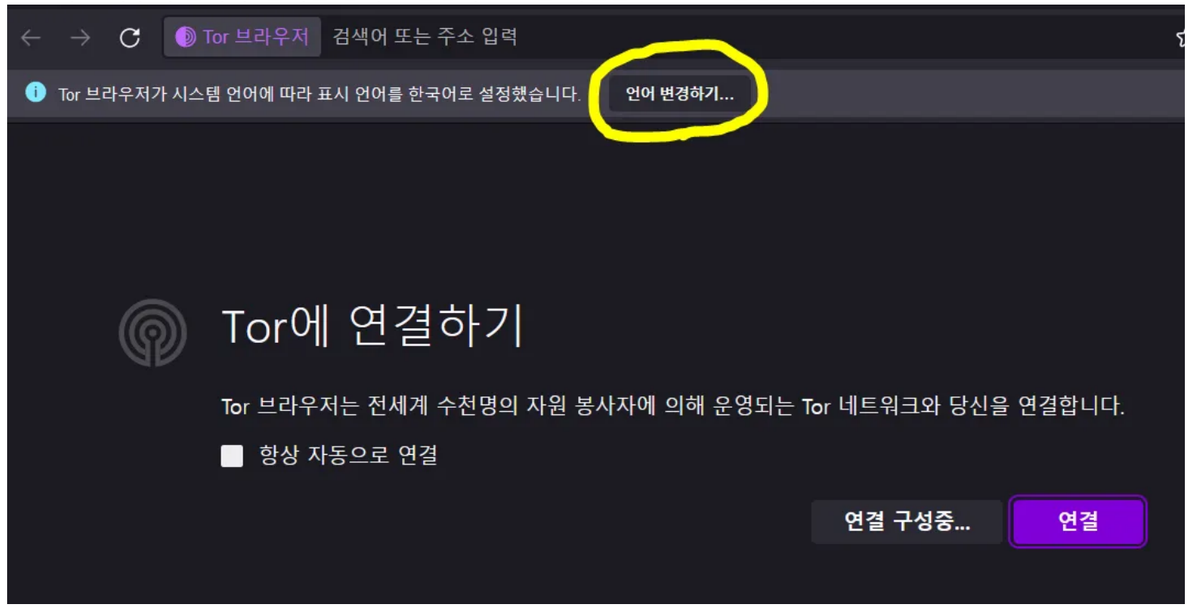
토어 브라우저를 세팅하여 Hyphanet을 이용해 보자.

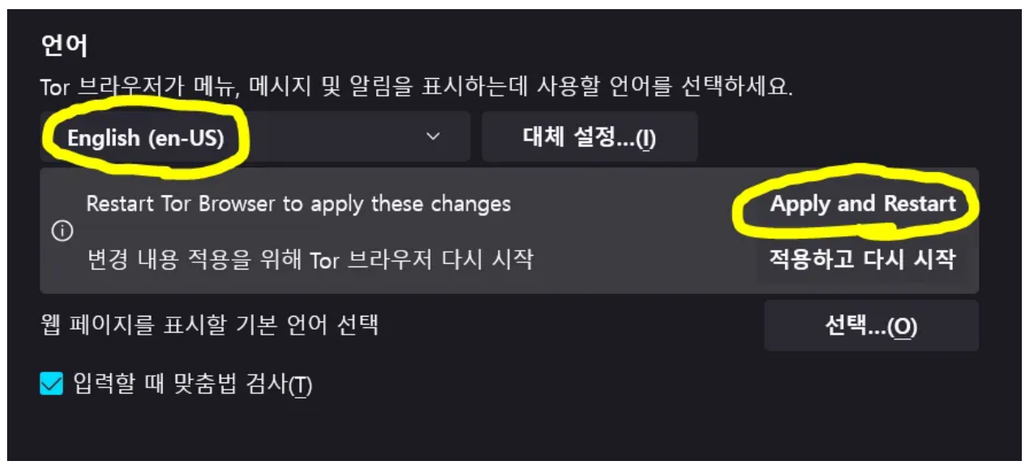
🔗토어 브라우저로 Hyphanet 사용하는법

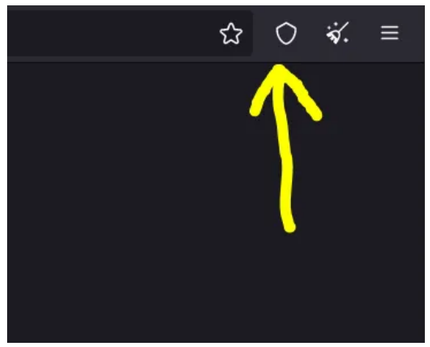
1. 🔗Hyphanet, 🔗Tor Browser 다운로드.

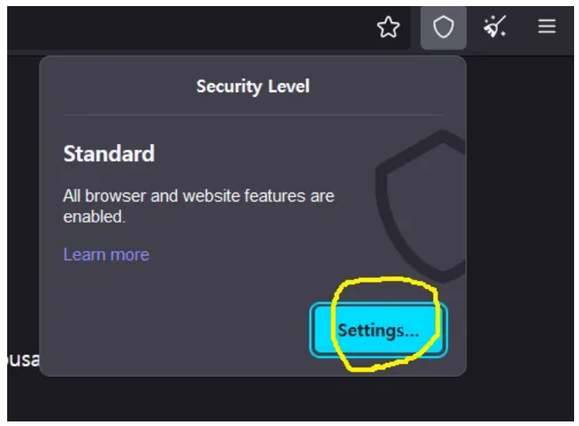


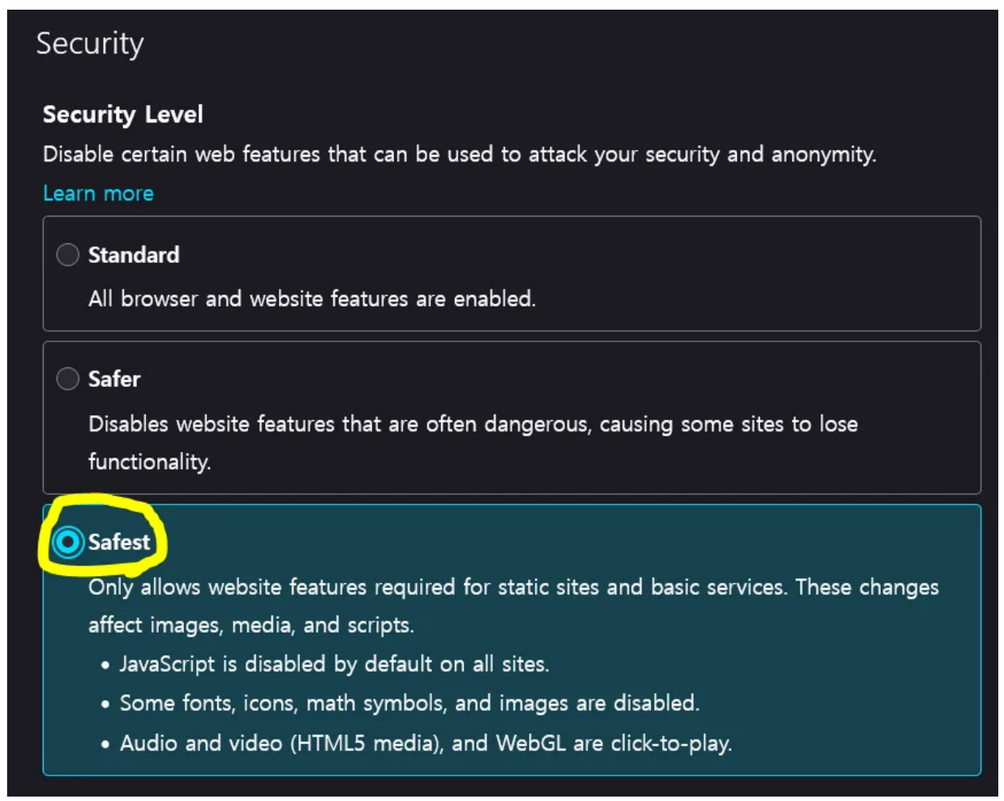
2. 토어 브라우저 설치 후 언어를 영어로 변경하고 보안 레벨을 Safest로 변경한다.


Tor 브라우저
검색어 또는 주소 입력
Tor 브라우저가 시스템 언어에 따라 표시 언어를 한국어로 설정했습니다.
언어 변경하기...
Tor에 연결하기
Tor 브라우저는 전세계 수천명의 자원 봉사자에 의해 운영되는 Tor 네트워크와 당신을 연결합니다.
항상 자동으로 연결
연결 구성중...
연결

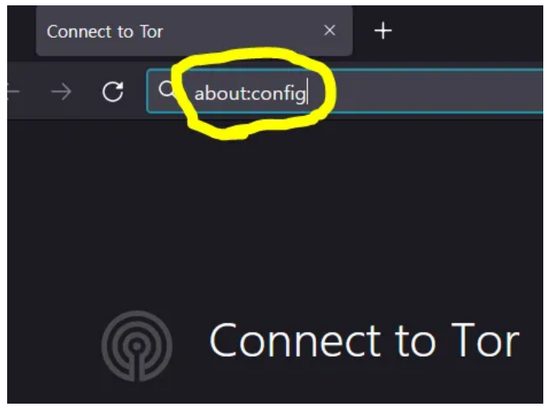

언어
Tor 브라우저가 메뉴, 메시지 및 알림을 표시하는데 사용할 언어를 선택하세요.
English (en-US)
대체 설정...(I)
Restart Tor Browser to apply these changes
Apply and Restart
변경 내용 적용을 위해 Tor 브라우저 다시 시작
적용하고 다시 시작
웹 페이지를 표시할 기본 언어 선택
선택...(O)
입력할 때 맞춤법 검사(T)



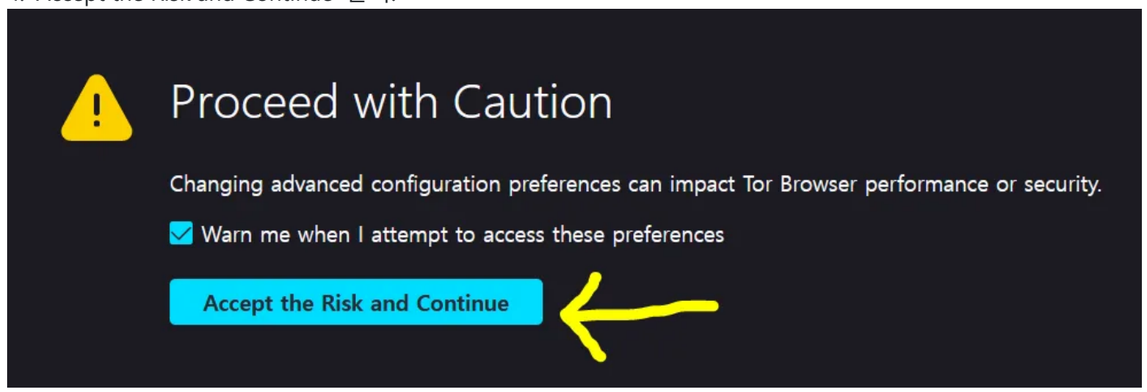



Security
Security Level
Disable certain web features that can be used to attack your security and anonymity.
Learn more
Standard
All browser and website features are enabled.
Safer
Disables website features that are often dangerous, causing some sites to lose functionality.
Safest
Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
• JavaScript is disabled by default on all sites.
• Some fonts, icons, math symbols, and images are disabled.
• Audio and video (HTML5 media), and WebGL are click-to-play.

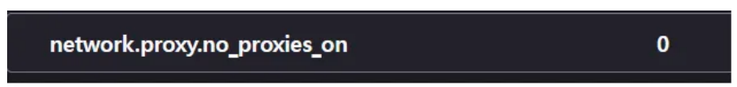
3. 주소창에 about:config 입력 후 엔터.

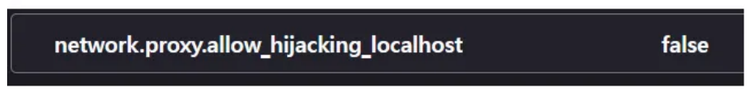


4. 'Accept the Risk and Continue' 클릭.

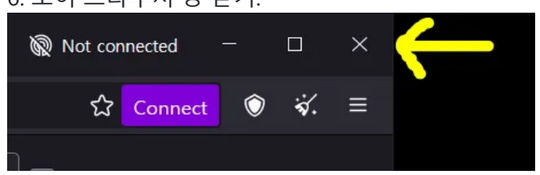

Proceed with Caution
Changing advanced configuration preferences can impact Tor Browser performance or security.
Warn me when I attempt to access these preferences
Accept the Risk and Continue

5. 아래와 같이 설정한다.
network.proxy.no_proxies_on - 0
network.proxy.allow_hijacking_localhost - false
출처 - https://www.whonix.org/wiki/Freenet

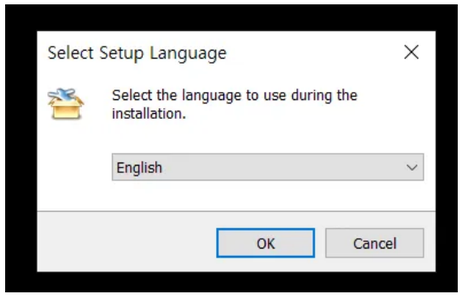


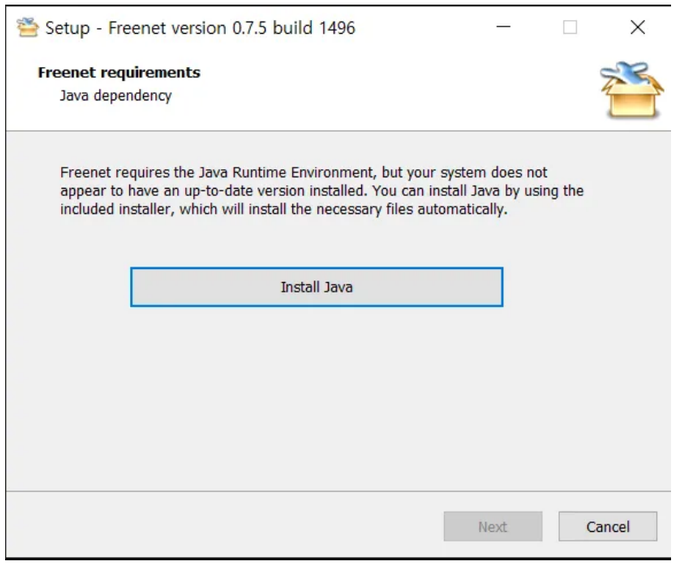


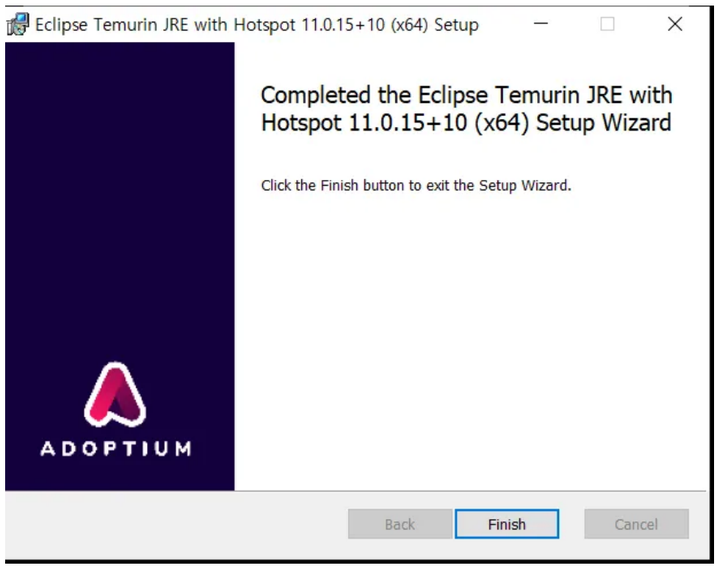
6. 토어 브라우저 창 닫기.

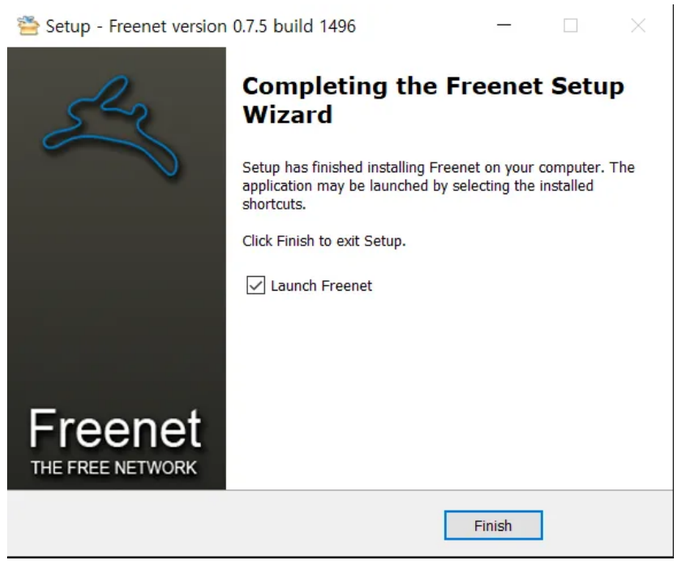


7. Hyphanet 설치. 설치과정에서 Java도 설치된다.

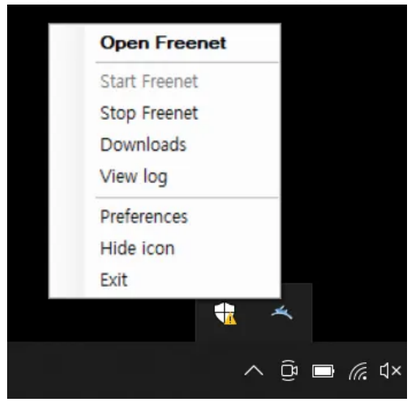






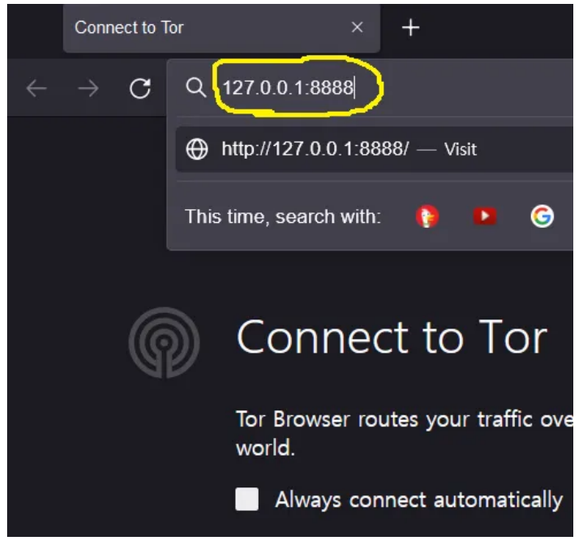


8. 바탕화면 오른쪽 아래에 아이콘이 생기는 것을 볼 수 있다.

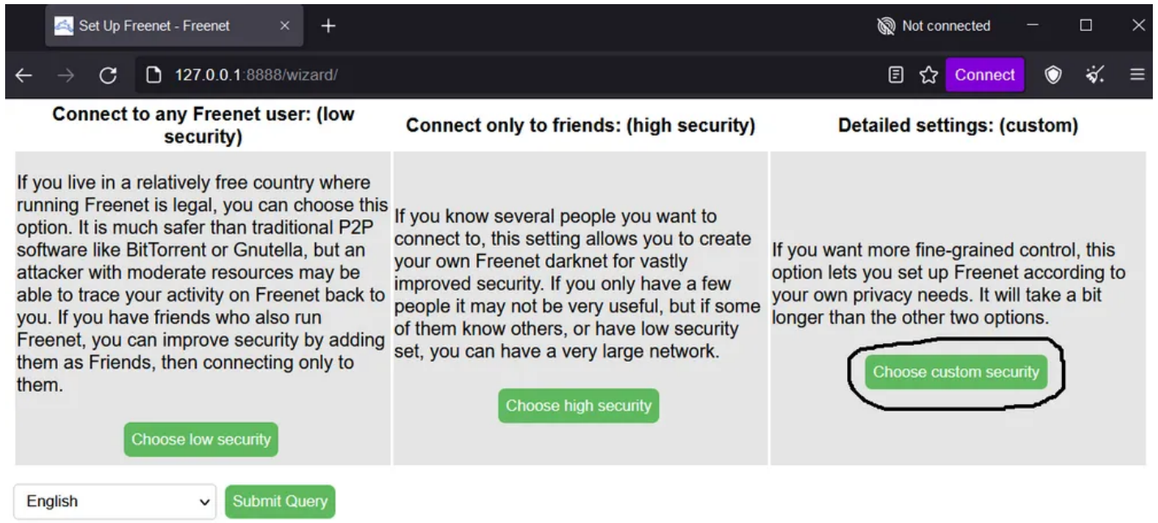


9. 엣지나 크롬 등 브라우저가 실행된다면 필요 없으므로 닫기.

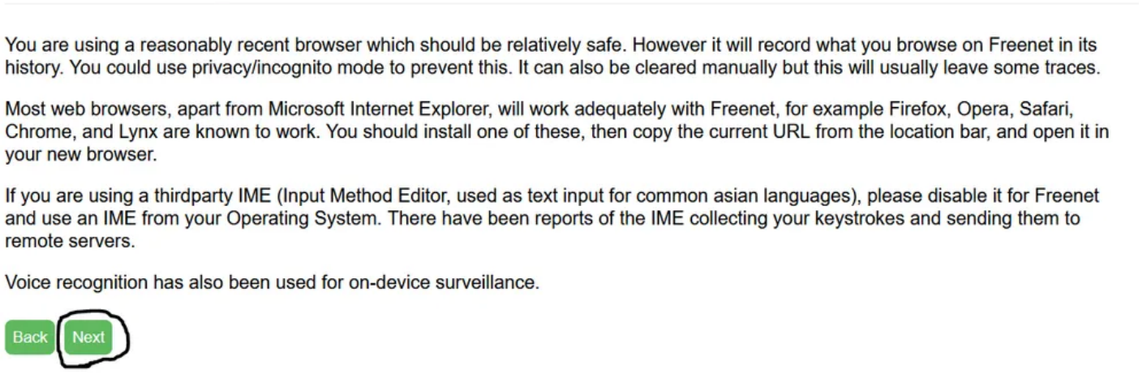
10. 토어 브라우저를 켜고 주소창에 127.0.0.1:8888 입력 후 엔터.



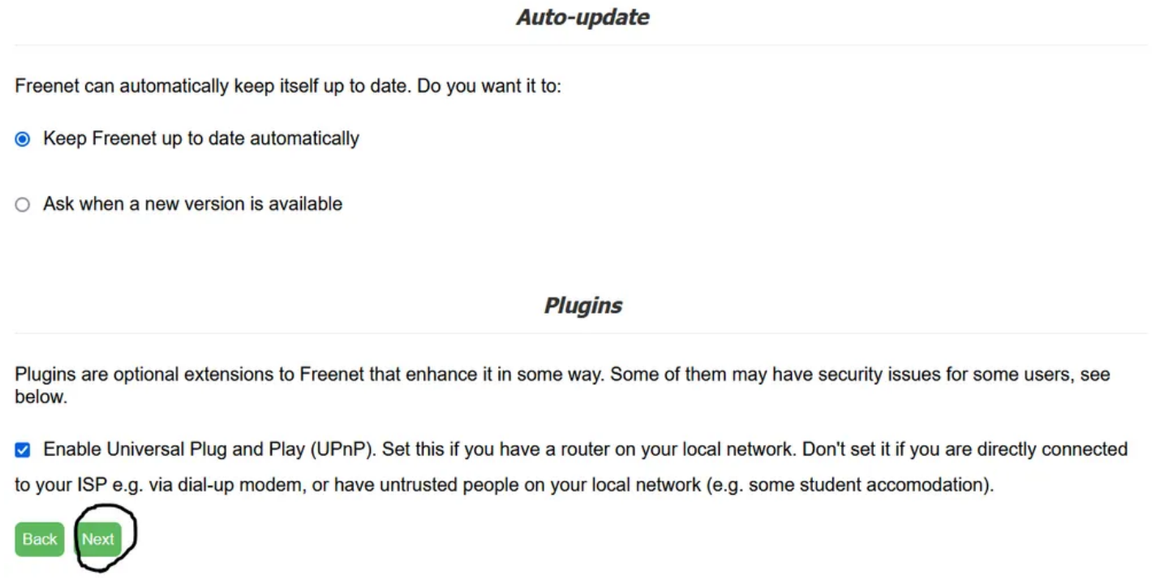
11. Choose custom security 클릭. Choose low security를 클릭하면 'Protection against a stranger attacking you over the internet(connect to strangers)'가 LOW로 선택되기 때문에 Choose custom security를 클릭하여 진행한다.
설정 구성에 참고한 글 - 참고 글 1, 참고 글 2


Set Up Freenet - Freenet
Not connected
127.0.0.1:8888/wizard/
Connect
Connect to any Freenet user: (low security)
Connect only to friends: (high security)
Detailed settings: (custom)
If you live in a relatively free country where running Freenet is legal, you can choose this option. It is much safer than traditional P2P software like BitTorrent or Gnutella, but an attacker with moderate resources may be able to trace your activity on Freenet back to you. If you have friends who also run Freenet, you can improve security by adding them as Friends, then connecting only to them.
Choose low security
If you know several people you want to connect to, this setting allows you to create your own Freenet darknet for vastly improved security. If you only have a few people it may not be very useful, but if some of them know others, or have low security set, you can have a very large network.
Choose high security
If you want more fine-grained control, this option lets you set up Freenet according to your own privacy needs. It will take a bit longer than the other two options.
Choose custom security
English
Submit Query

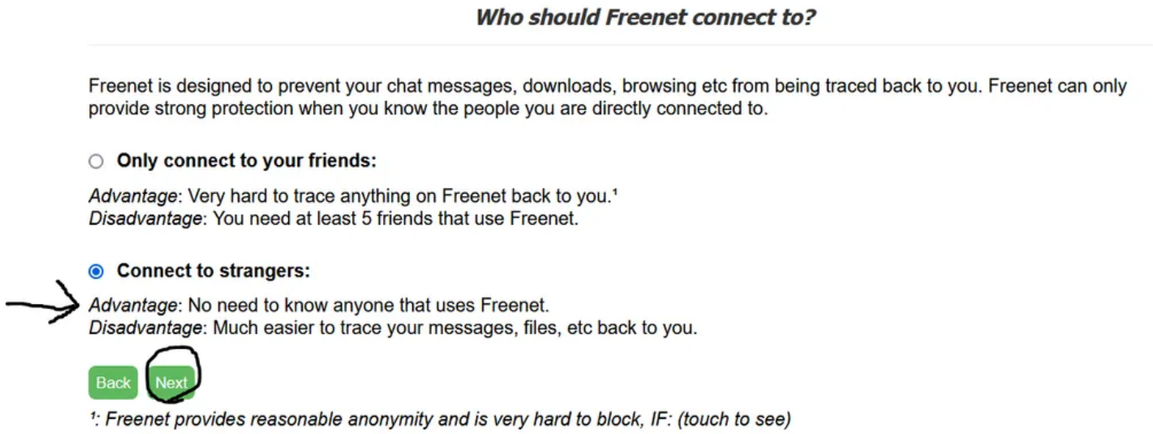
12. Next 클릭.


You could use privacy mode or a separate browser to improve security
You are using a reasonably recent browser which should be relatively safe. However it will record what you browse on Freenet in its history. You could use privacy/incognito mode to prevent this. It can also be cleared manually but this will usually leave some traces.
Most web browsers, apart from Microsoft Internet Explorer, will work adequately with Freenet, for example Firefox, Opera, Safari, Chrome, and Lynx are known to work. You should install one of these, then copy the current URL from the location bar, and open it in your new browser.
If you are using a thirdparty IME (Input Method Editor, used as text input for common asian languages), please disable it for Freenet and use an IME from your Operating System. There have been reports of the IME collecting your keystrokes and sending them to remote servers.
Voice recognition has also been used for on-device surveillance.
Back
Next

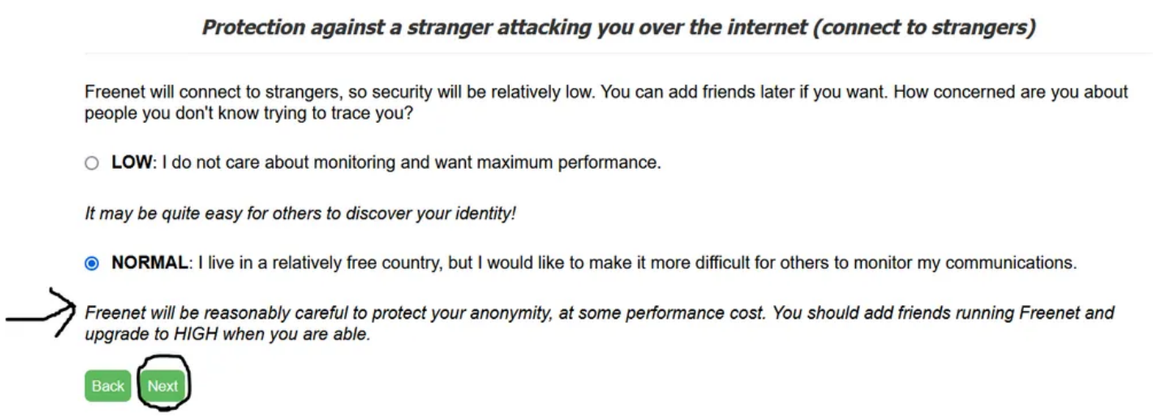
13. Next 클릭.


Auto-update
Freenet can automatically keep itself up to date. Do you want it to:
Keep Freenet up to date automatically
Ask when a new version is available
Plugins
Plugins are optional extensions to Freenet that enhance it in some way. Some of them may have security issues for some users, see below.
Enable Universal Plug and Play (UPnP). Set this if you have a router on your local network. Don't set it if you are directly connected to your ISP e.g. via dial-up modem, or have untrusted people on your local network (e.g. some student accomodation).
Back
Next

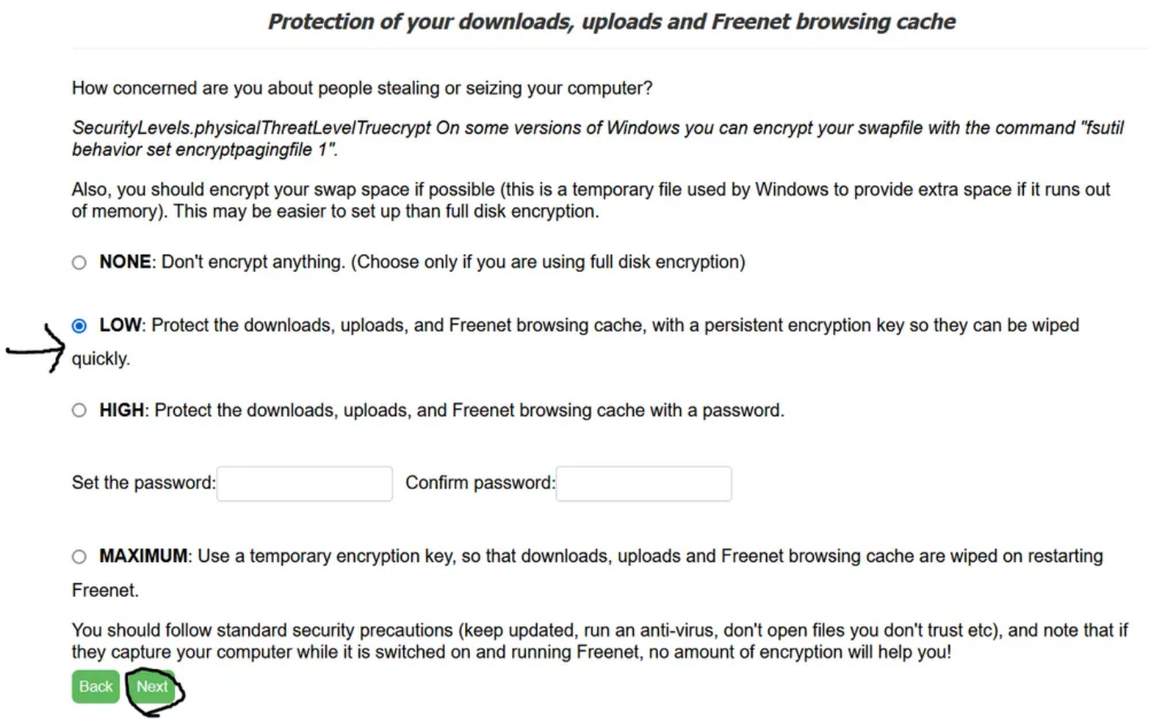
14. Connect to strangers 선택 후 Next 클릭.


Who should Freenet connect to?
Freenet is designed to prevent your chat messages, downloads, browsing etc from being traced back to you. Freenet can only provide strong protection when you know the people you are directly connected to.
Only connect to your friends:
Advantage: Very hard to trace anything on Freenet back to you.[1]
Disadvantage: You need at least 5 friends that use Freenet.
Connect to strangers:
Advantage: No need to know anyone that uses Freenet.
Disadvantage: Much easier to trace your messages, files, etc back to you.
Back
Next
[1]: Freenet provides reasonable anonymity and is very hard to block, IF: (touch to see)

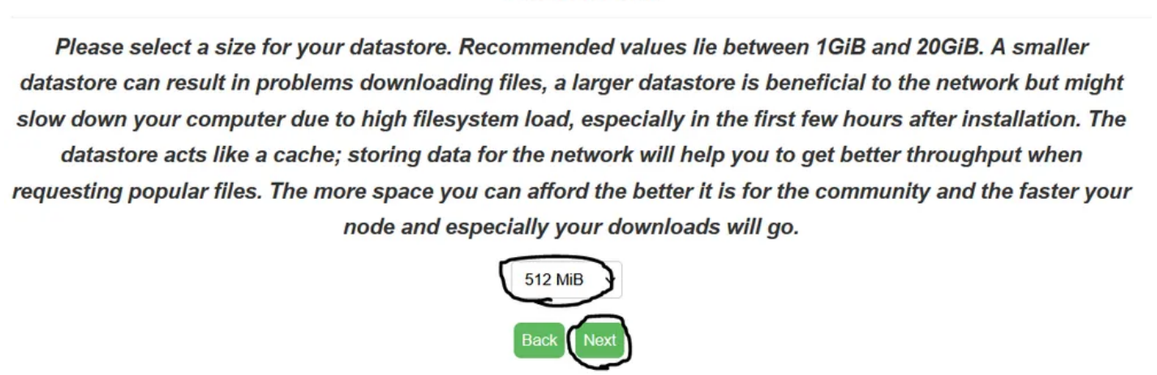
15. NORMAL 선택 후 Next 클릭.


Protection against a stranger attacking you over the internet (connect to strangers)
Freenet will connect to strangers, so security will be relatively low. You can add friends later if you want. How concerned are you about people you don't know trying to trace you?
LOW: I do not care about monitoring and want maximum performance.
It may be quite easy for others to discover your identity!
NORMAL: I live in a relatively free country, but I would like to make it more difficult for others to monitor my communications.
Freenet will be reasonably careful to protect your anonymity, at some performance cost. You should add friends running Freenet and upgrade to HIGH when you are able.
Back
Next

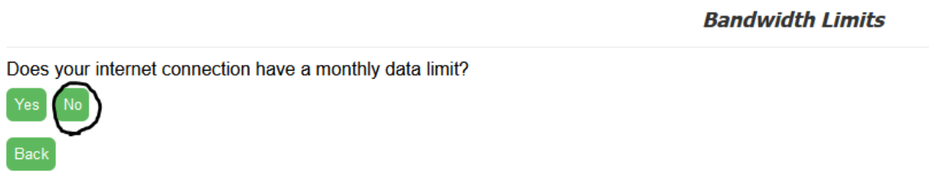
16. LOW 선택 후 Next 클릭.



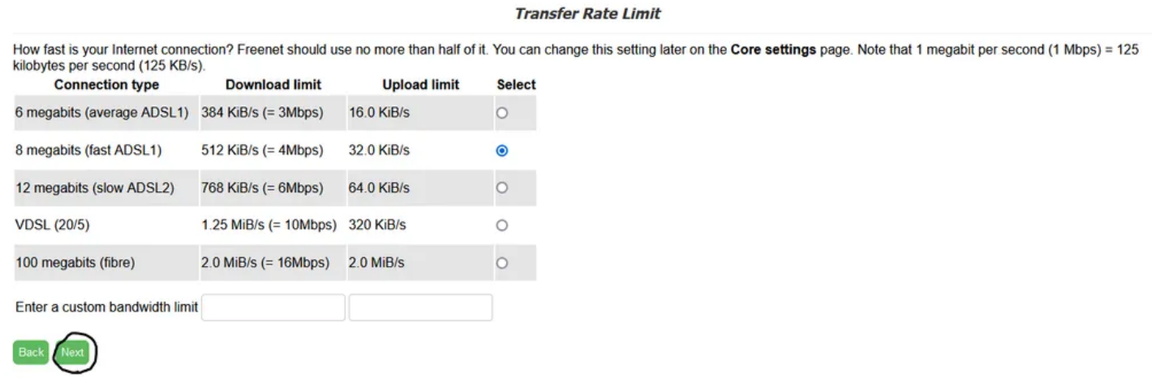
17. 512MB 선택 후 Next 클릭.



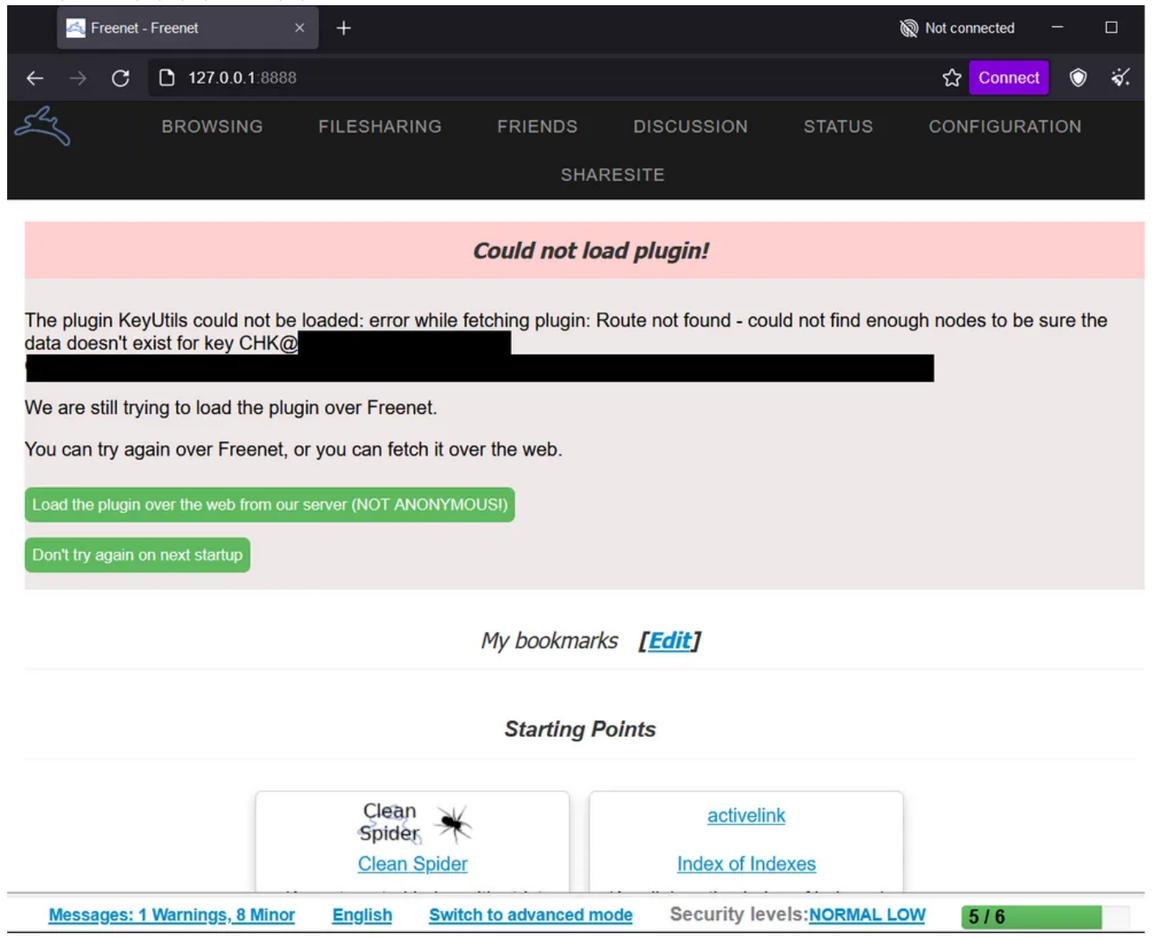
18. No 클릭.

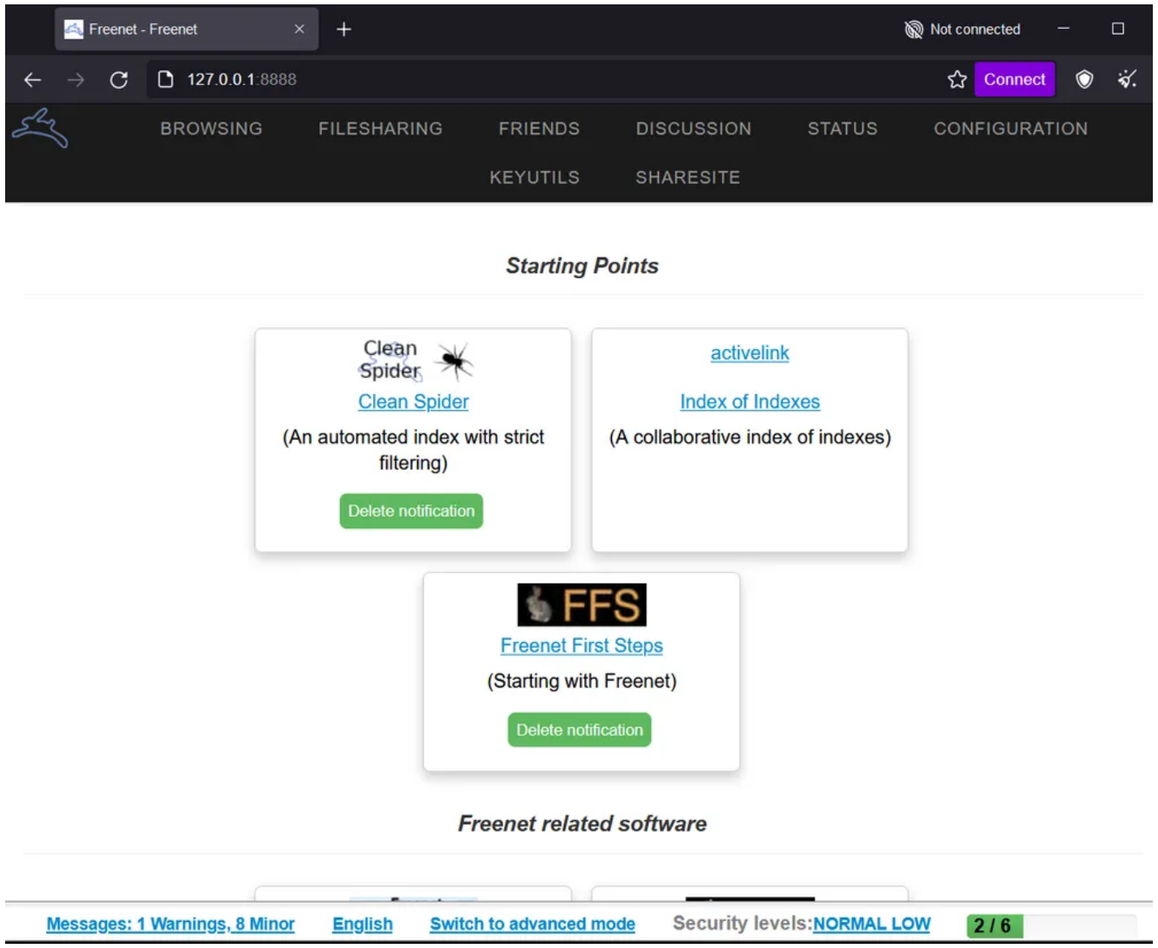


19. Next 클릭.

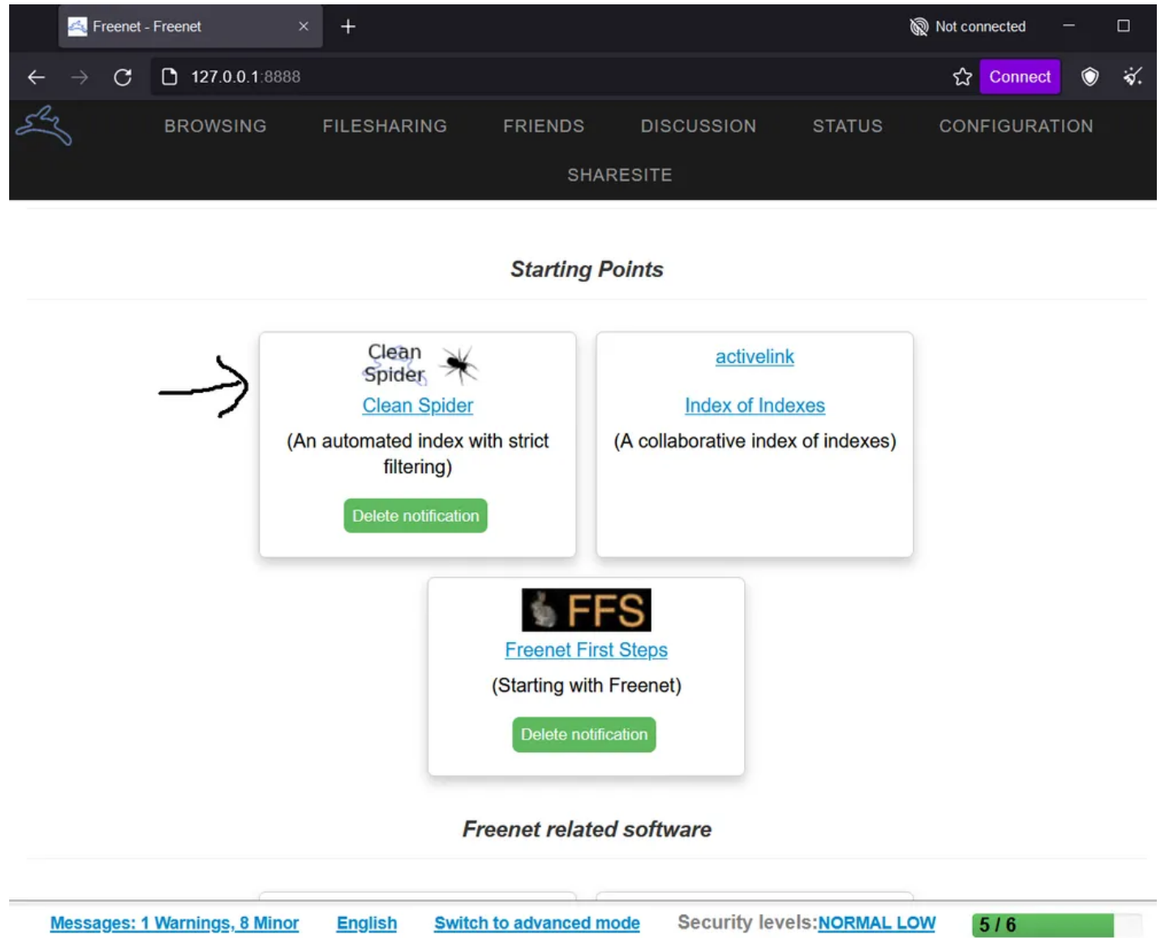


20. 메인 홈페이지의 모습이다.

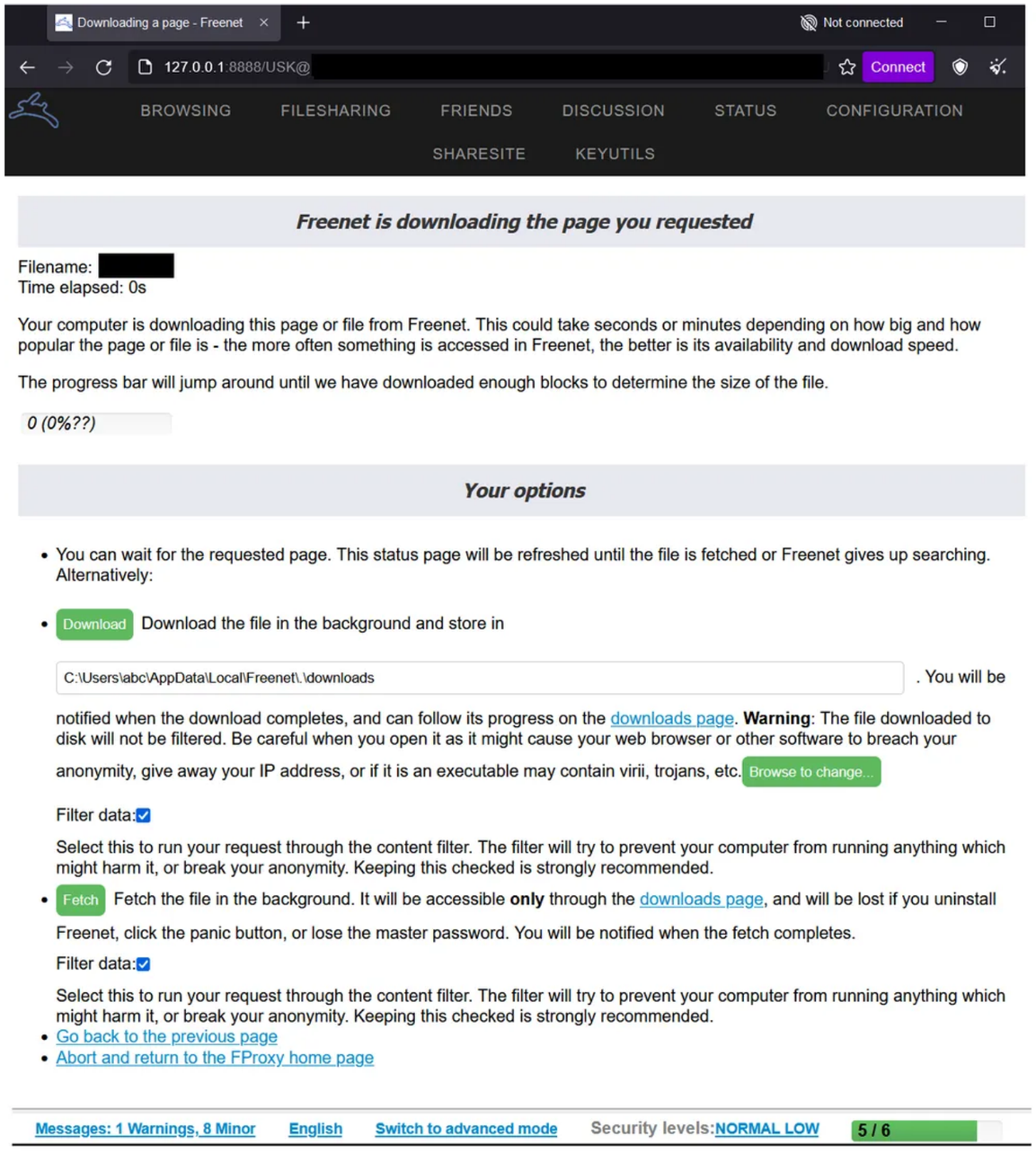




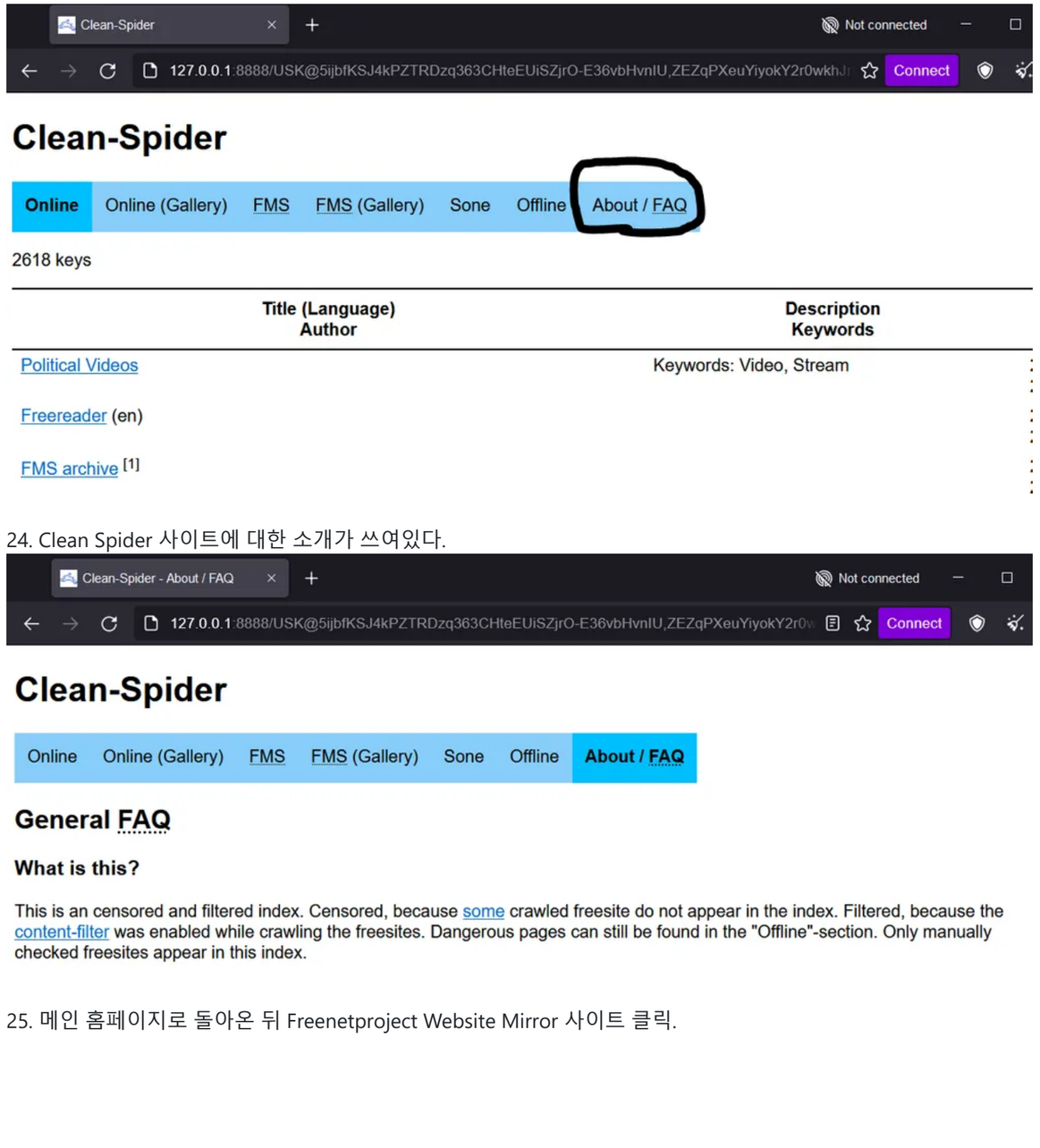
21. Clean Spider 사이트 클릭.



22. 그냥 기다리면 된다. 사이트를 탐방하면서 아래의 이미지를 매번 보게 될 것이다.


Downloading a page - Freenet
Not connected
127.0.0.1:8888/USK@
Connect
BROWSING
FILESHARING
FRIENDS
DISCUSSION
STATUS
CONFIGURATION
SHARESITE
KEYUTILS
Freenet is downloading the page you requested
Filename:
Time elapsed: 0s
Your computer is downloading this page or file from Freenet. This could take seconds or minutes depending on how big and how popular the page or file is - the more often something is accessed in Freenet, the better is its availability and download speed.
The progress bar will jump around until we have downloaded enough blocks to determine the size of the file.
0 (0%??)
Your options
You can wait for the requested page. This status page will be refreshed until the file is fetched or Freenet gives up searching. Alternatively:
Download
Download the file in the background and store in
C:\Users\abc\AppData\Local\Freenet\.\downloads
. You will be notified when the download completes, and can follow its progress on the downloads page. Warning: The file downloaded to disk will not be filtered. Be careful when you open it as it might cause your web browser or other software to breach your anonymity, give away your IP address, or if it is an executable may contain virii, trojans, etc.
Browse to change...
Filter data:
Select this to run your request through the content filter. The filter will try to prevent your computer from running anything which might harm it, or break your anonymity. Keeping this checked is strongly recommended.
Fetch
Fetch the file in the background. It will be accessible only through the downloads page, and will be lost if you uninstall Freenet, click the panic button, or lose the master password. You will be notified when the fetch completes.
Filter data:
Select this to run your request through the content filter. The filter will try to prevent your computer from running anything which might harm it, or break your anonymity. Keeping this checked is strongly recommended.
Go back to the previous page
Abort and return to the FProxy home page
Messages: 1 Warnings, 8 Minor
English
Switch to advanced mode
Security levels:NORMAL LOW
5 / 6

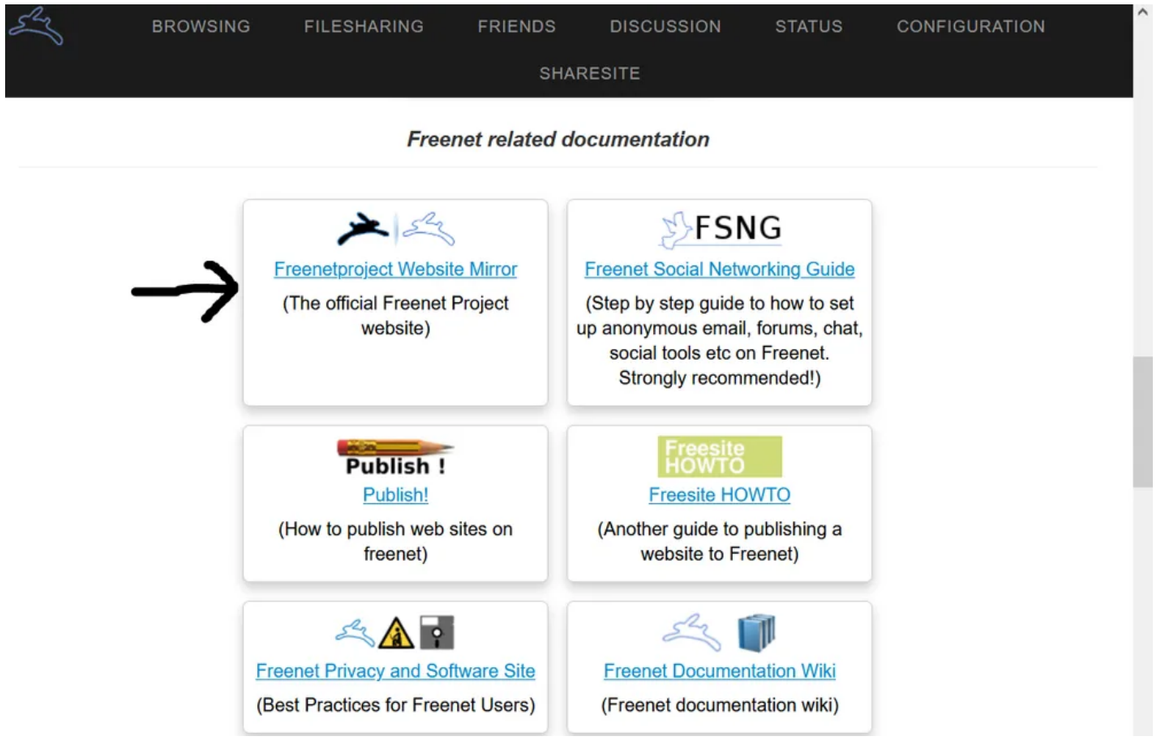
23. 보다시피 사이트 UI가 투박하다. About/FAQ 클릭.



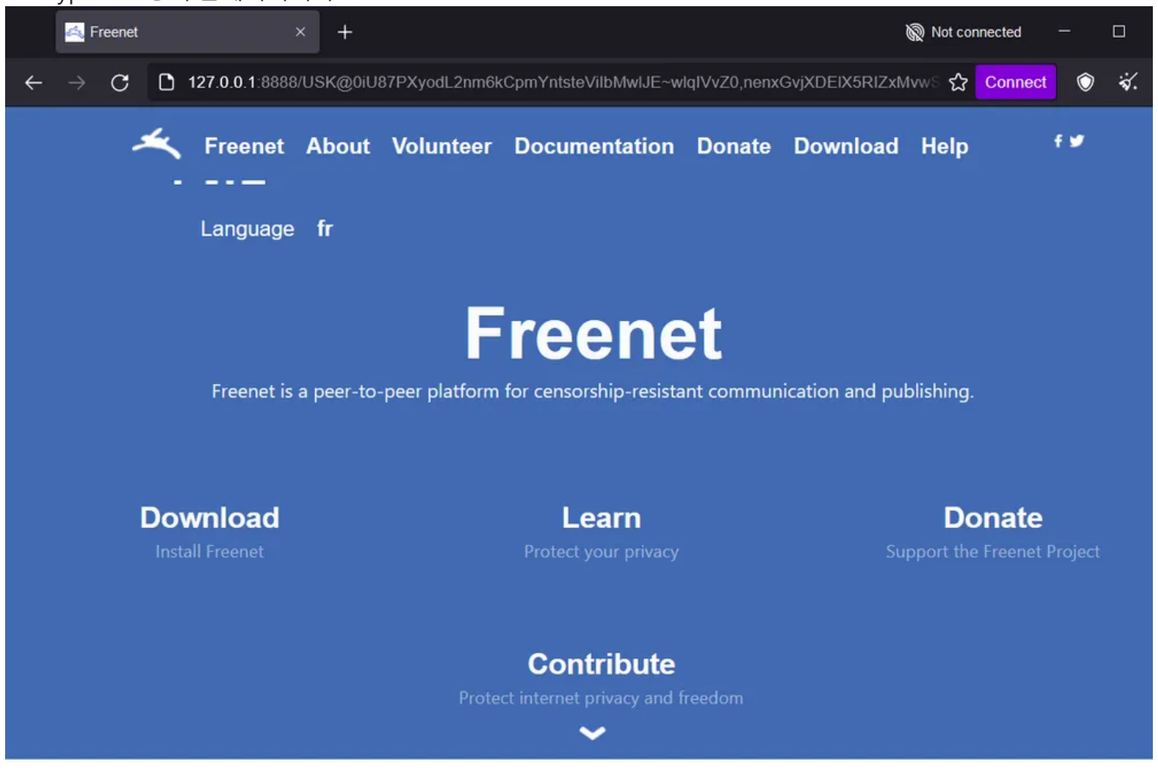
24. Clean Spider 사이트에 대한 소개가 쓰여있다.

Clean-Spider - About / FAQ
Not connected
127.0.0.1:8888/USK@5ijbfKSJ4kPZTRDzq363CHteEUiSZjrO-E36vbHvnIU,ZEZqPXeuYiyokY2r0w
Connect
Clean-Spider
Online
Online (Gallery)
FMS
FMS (Gallery)
Sone
Offline
About / FAQ
General FAQ
What is this?
This is an censored and filtered index. Censored, because some crawled freesite do not appear in the index. Filtered, because the content-filter was enabled while crawling the freesites. Dangerous pages can still be found in the "Offline"-section. Only manually checked freesites appear in this index.

25. 메인 홈페이지로 돌아온 뒤 Freenetproject Website Mirror 사이트 클릭.



26. Hyphanet 공식 홈페이지이다.



지금까지 토어 브라우저를 세팅하여 Hyphanet을 이용하는 방법을 알아보았다.

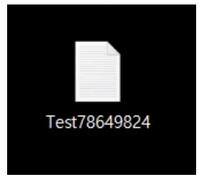
4.3. 파일을 공유하는 법

Hyphanet으로 파일을 공유하는 법

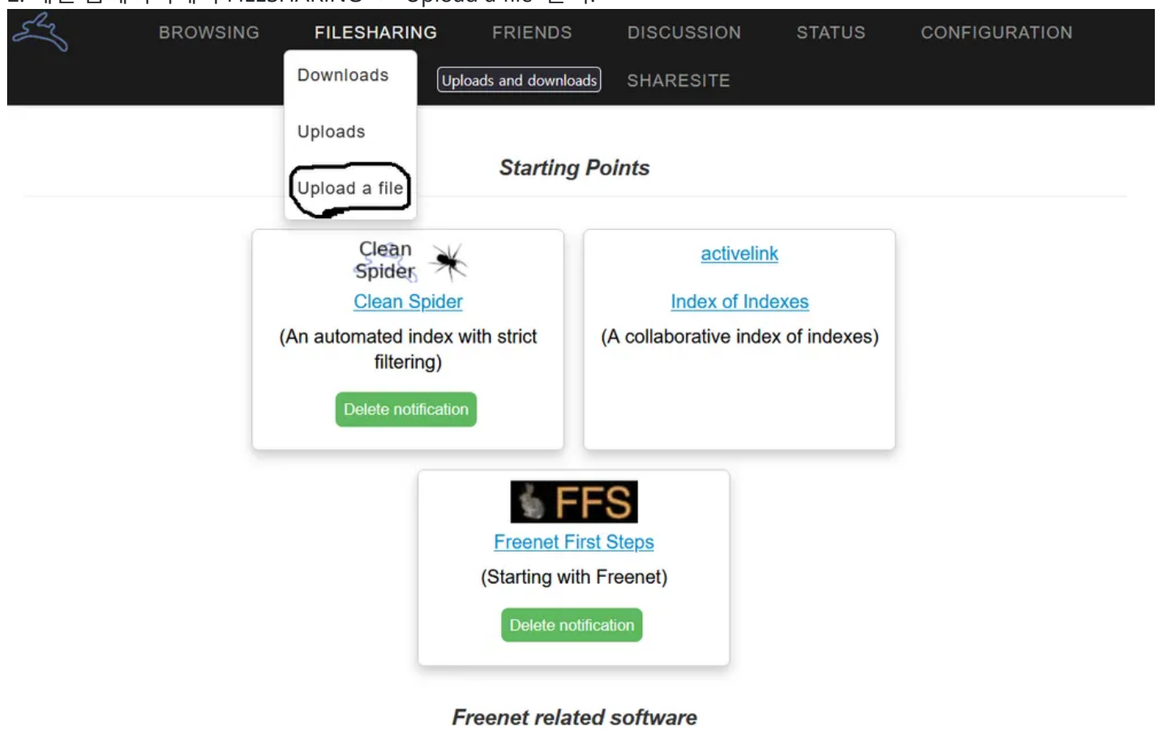
Hyphanet으로 파일을 공유하는 법을 설명한다. 파일 공유 전 하기 주의사항을 정독하기 바란다.

- Hyphanet에 한번 올린 파일은 게시자조차 삭제가 불가능하다. 파일이 삭제되는 유일한 방법은 그 파일이 인기가 없어 그 파일을 찾는 사람이 아무도 없어지는 것뿐이다. 그러므로 파일을 업로드하기 전에 이 파일이 올려도 되는 파일인지 신중을 기해야 한다.
- Hyphanet을 사용하여 저작권이 있는 자료를 원작자 허가 없이 업로드하는 것은 불법 공유, 즉 범죄에 해당된다.

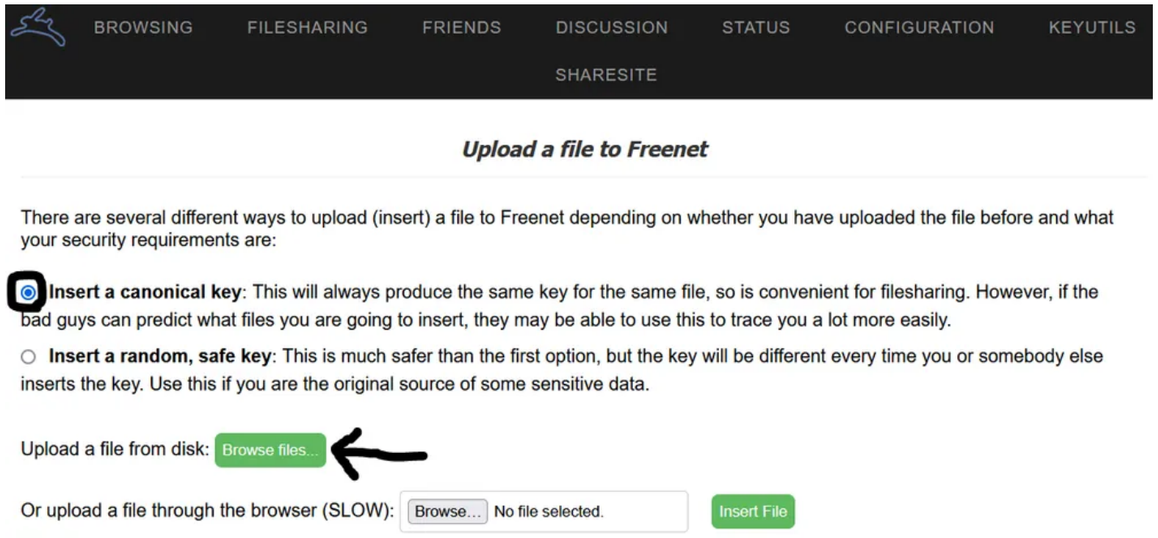
1. 테스트용으로 파일을 하나 만든다. 여기서는 바탕화면에 Test78649824.txt라는 파일을 만들었다.



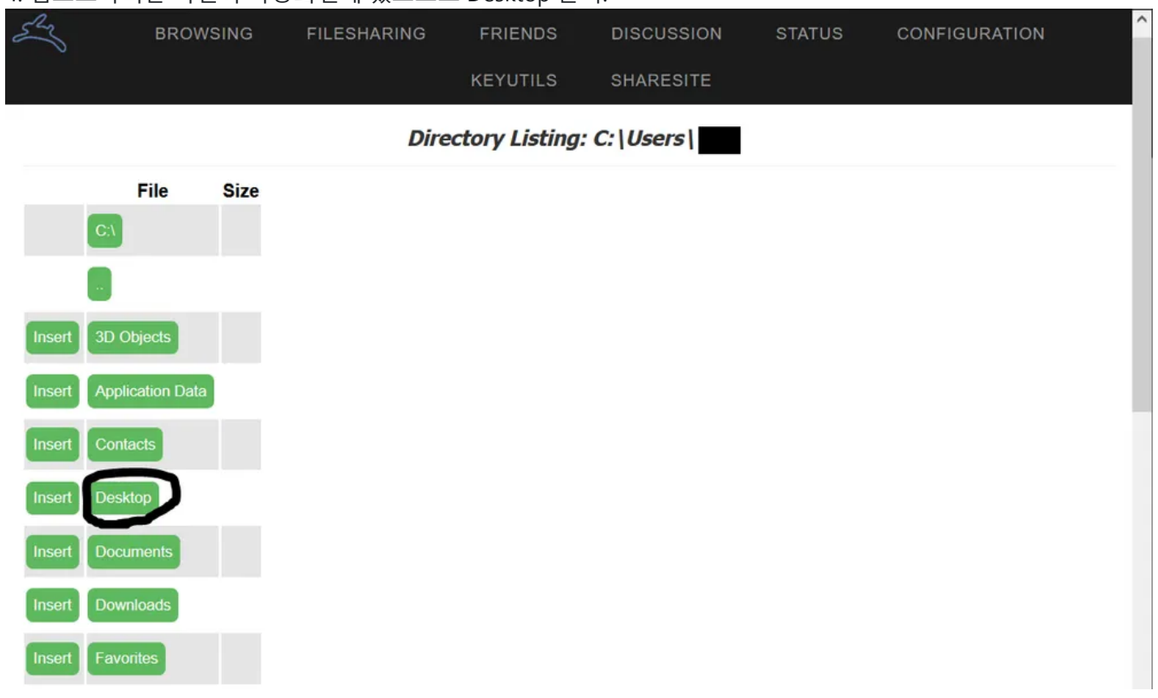
2. 메인 홈페이지에서 FILESHARING -> 'Upload a file' 클릭.



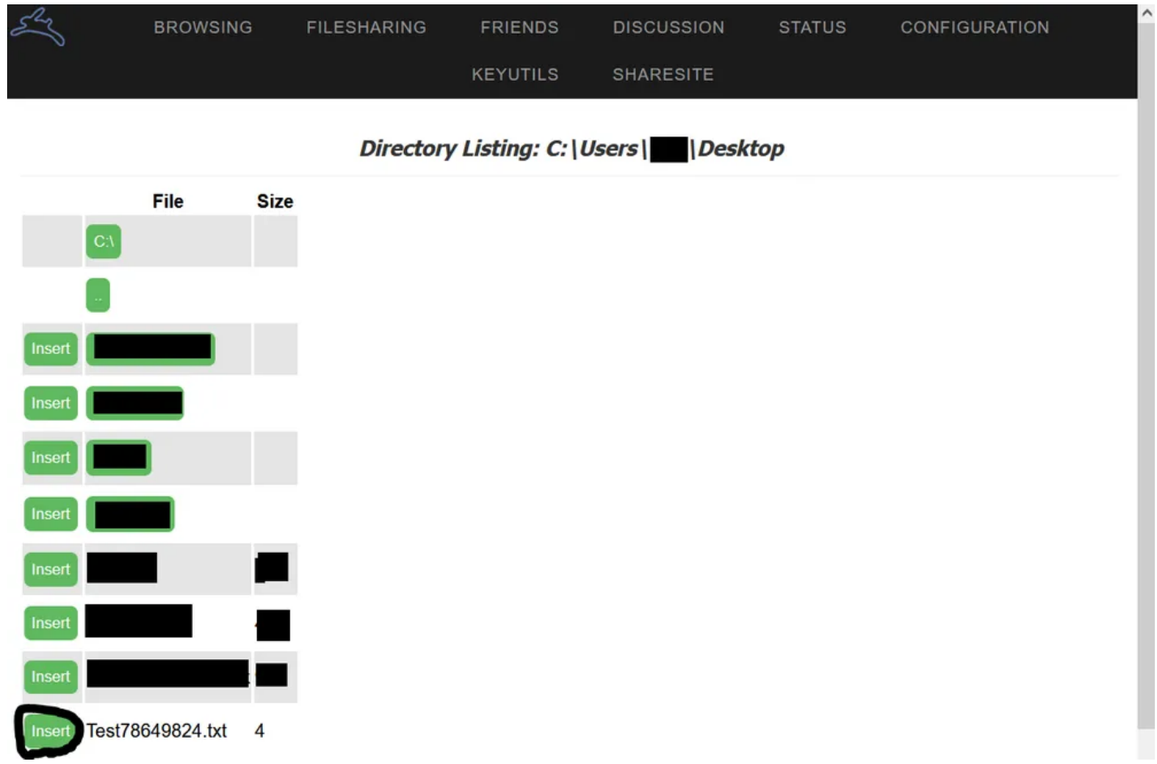
3. 'Insert a canonical key' 선택 후 'Upload a file from disk'의 'Browse files' 클릭.



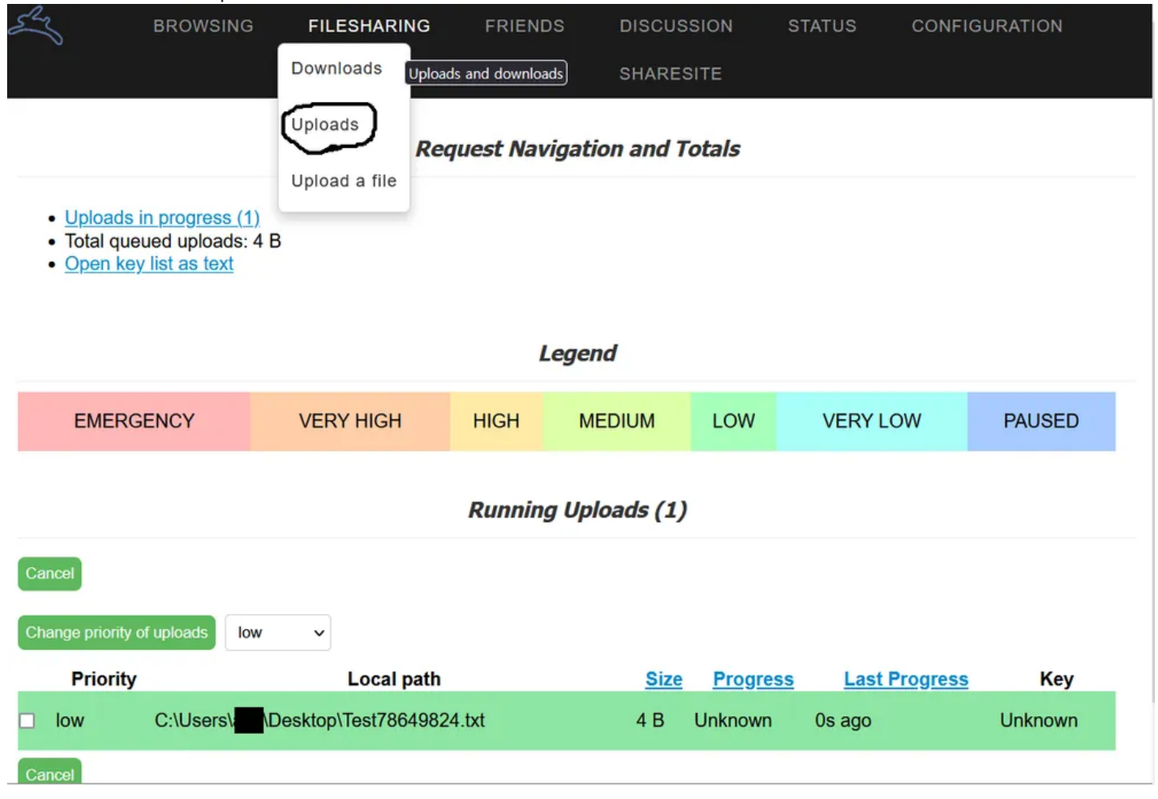
4. 업로드하려는 파일이 바탕화면에 있으므로 Desktop 클릭.



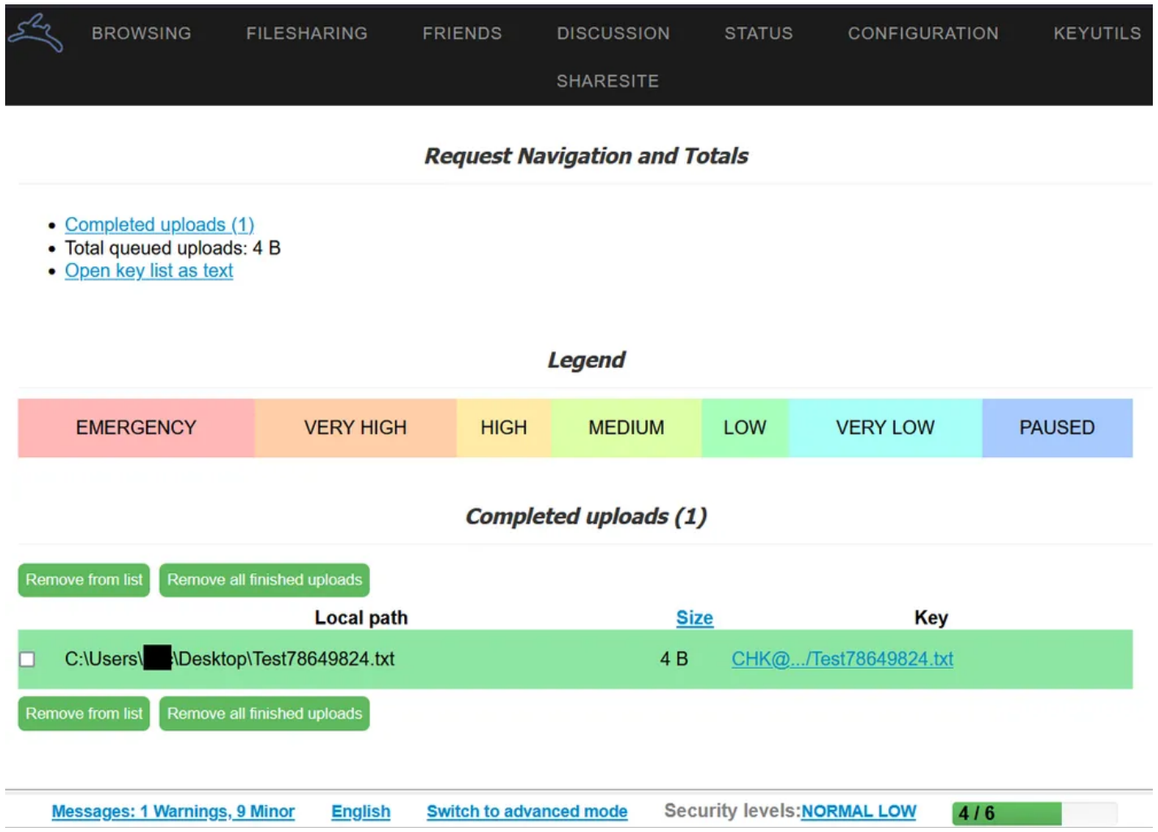
5. 업로드하려는 파일 옆의 Insert 클릭.



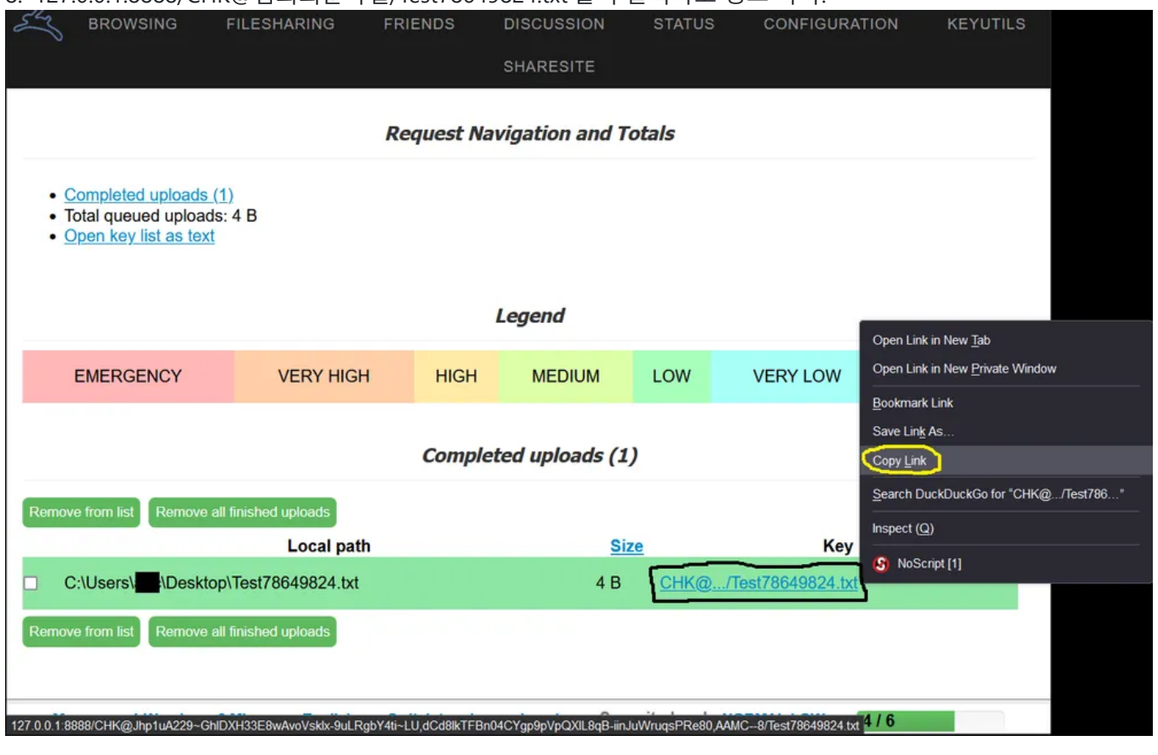
6. FILESHARING -> Uploads 클릭.



7. 파일 업로드가 완료되었다.



8. '127.0.0.1:8888/CHK@임의의문자열/Test78649824.txt'를 우클릭하고 링크 복사.



9. '127.0.0.1:8888/CHK@임의의문자열/Test78649824.txt'에서 'CHK@임의의문자열/Test78649824.txt'가 파일의 키(Key)이다.

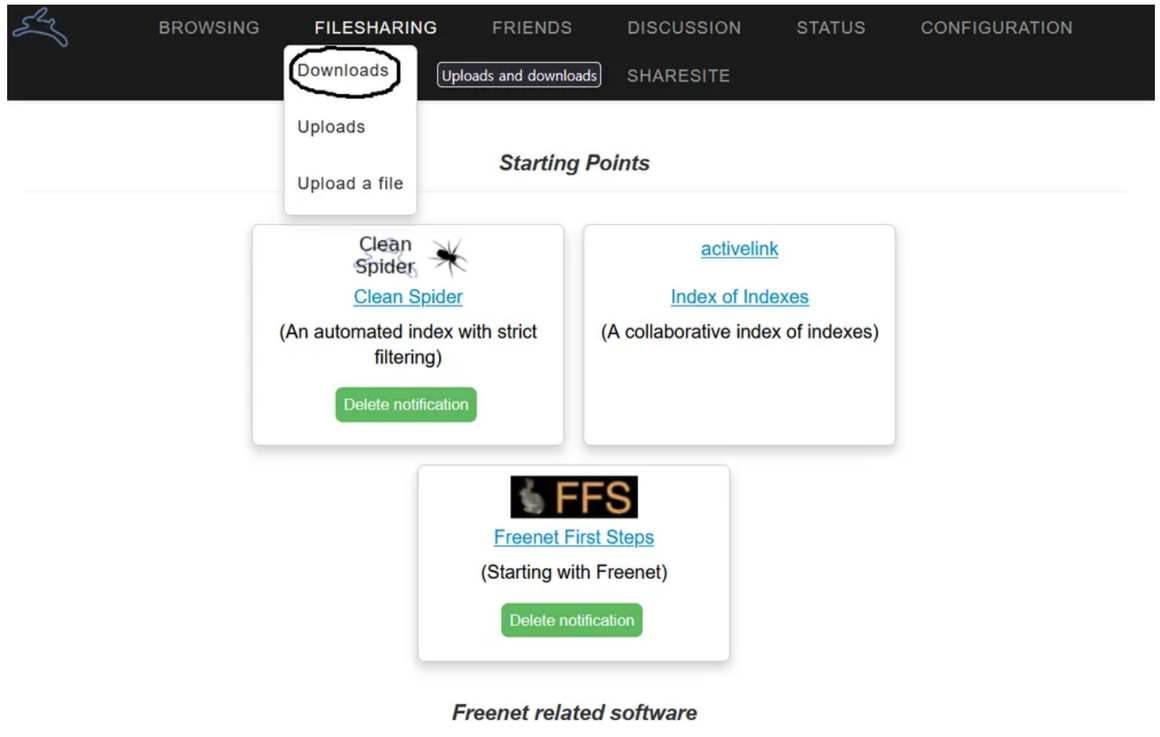
복사한 링크 주소
http://127.0.0.1:8888/CHK@임의의문자열/Test78649824.txt

키
CHK@임의의문자열/Test78649824.txt

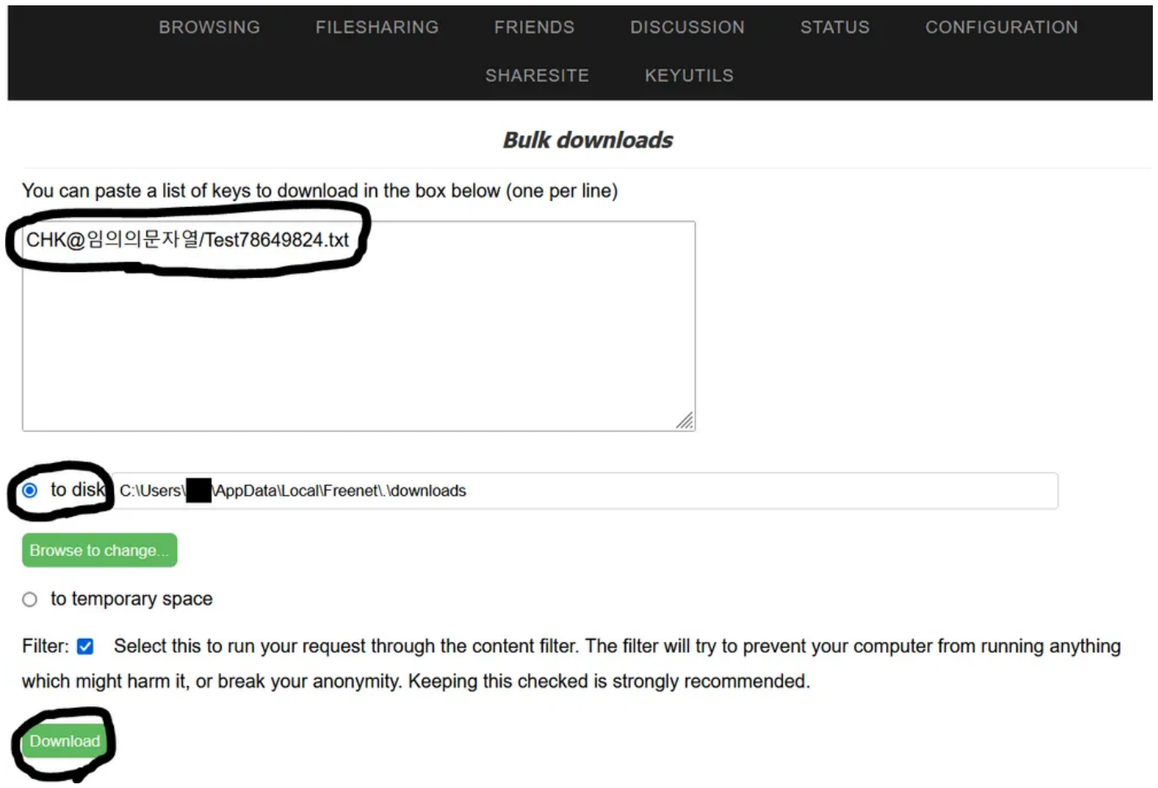
10. 파일을 공유하려는 사람에게 파일의 키(Key)를 알려준다.

철수: Test78649824.txt라는 파일 공유 부탁해요
영희: Freenet에 올렸어요
영희: CHK@임의의문자열/Test78649824.txt
철수: 고마워요

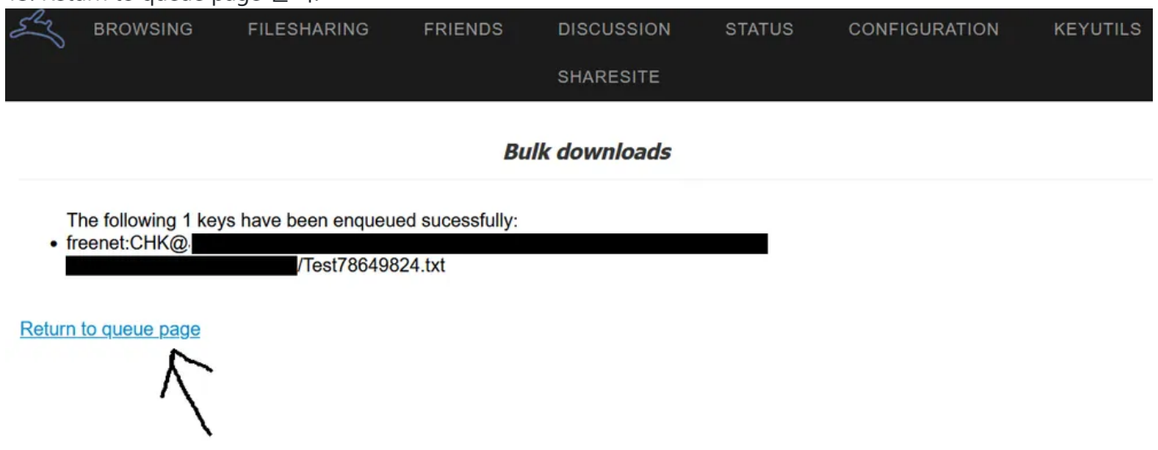
11. FILESHARING -> Downloads 클릭.



12. 파일의 키(Key)를 입력하고, 'to disk'를 선택한 뒤, Download 클릭.

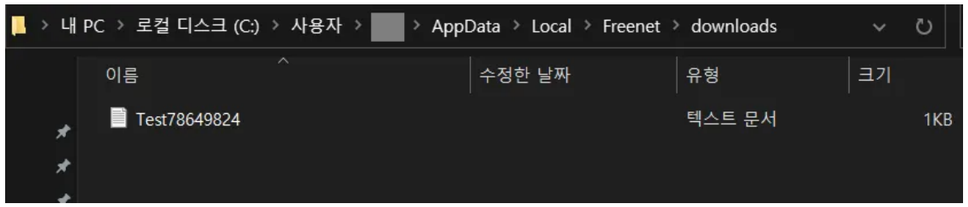


13. Return to queue page 클릭.



14. 파일 다운로드가 완료되었다.

15. 다운받은 파일을 확인한다.



지금까지 Hyphanet으로 파일을 공유하는 방법을 알아보았다.

4.4. FMS(Freenet Message System) 사용법

주의사항
1. Hyphanet의 특성상 FMS에 한번 올린 글은 게시자조차 삭제가 불가능하다. 그러므로 글을 업로드하기 전에 이 글이 올려도 되는 글인지 신중을 기해야 한다.
2. 위 가이드의 작성자는 FMS에 대한 이해가 매우 빈약하다. 그러므로 만약 다른 사람의 글과 위 가이드의 내용이 충돌한다면 위 가이드가 틀린 내용이라고 여기는 것이 좋다. 교차검증을 하자.

🔗 https://www.draketo.de/english/freenet/friendly-communication-with-anonymity 🔗 @
🔗 https://www.reddit.com/r/Freenet/comments/1q3oyt6/what_is_the_point_of_identity_announcement/ 🔗 @

🔗 Hyphanet FMS(Freenet Message System) 사용법
🔗 Hyphanet FMS(Freenet Message System)에서 상대방 평가하는 법
🔗 FMS(Freenet Message System)에 대한 설명
🔗 FMS Trust System FAQ (English version)
🔗 FMS Trust System example (English version)
🔗 FMS 신뢰 시스템 FAQ (Korean version)
🔗 FMS 신뢰 시스템 예시 (Korean version)

FMS를 통해 Hyphanet에서 포럼을 만들 수 있다.

FMS와 Frost에서는 글을 써도 바로 보드에 등록되지 않고 기다려야 한다.
첫글은 'Announce Identity' 메뉴에서 캡챠를 2~3번 정도 푼 뒤 5~6시간 정도 기다리면 보드에 글이 등록된다. 두 번째 글 및 댓글부터는 15~20분 정도 기다리면 보드에 글 및 댓글이 등록된다.

FMS의 글들을 아카이브해놓은 FMSArchive라는 사이트를 보면 좋다. 다양한 주제의 포럼을 볼 수 있다.🔗 관련 링크

4.5. Frost-Next 사용법

주의사항
1. Hyphanet의 특성상 Frost-Next에 한번 올린 글은 게시자조차 삭제가 불가능하다. 그러므로 글을 업로드하기 전에 이 글이 올려도 되는 글인지 신중을 기해야 한다.
2. Frost-Next를 설치하는 과정에서 'Import General'을 선택하면 위험한 주제의 보드가 추가되지 않으므로 꼭 'Import General'을 선택하기를 권장한다.
3. 위 가이드의 작성자는 Frost-Next에 대한 이해가 매우 빈약하다. 그러므로 만약 다른 사람의 글과 위 가이드의 내용이 충돌한다면 위 가이드가 틀린 내용이라고 여기는 것이 좋다. 교차검증을 하자.

Frost의 개량판인 Frost-Next를 통해서 Hyphanet에서 포럼을 만들 수 있다. 🔗 Hyphanet Frost-Next 사용 방법

FMS와 Frost에서는 글을 써도 바로 보드에 등록되지 않고 기다려야 한다.
글 및 댓글을 쓴 뒤 10~15분 정도 기다리면 보드에 글 및 댓글이 등록된다.

4.6. Hyphanet 클라이언트 설정법

"wrapper.conf"나 "freenet.ini"를 메모장에서 불러서 해당 숫자나 문구로 변경하고 저장한다.

4.6.1. wrapper 폴더 안의 "wrapper.conf" 파일 설정

· wrapper.java.maxmemory = 512
· wrapper.console.loglevel = NONE
· wrapper.syslog.loglevel = NONE

※ 64bit 버전의 Java로 Hyphanet을 실행하는 경우
· wrapper.java.command = "경로"

Windows의 Hyphanet은 wrapper.conf의 wrapper.java.command에 64bit 버전의 "java"의 전체 경로를 지정할 필요가 있다. 기본적으로 32bit 버전의 Java의 경로를 레지스트리에서 검색할 수 있도록 만들어져 있는 것 같지만, 64bit 버전에서 동작시키고 싶은 경우는 "경로"에 Java가 설치되어 있는 경로 (예 : `C:\Program Files\Java\jre6\bin\java`)를 직접 지정하자.

4.6.2. Hyphanet 폴더 안의 "freenet.ini" 파일 설정

· node.load.threadLimit = 1024

RAMDisk를 가지고 있고, RAMDisk가 1GB 여유가 있다면,
· node.tempDir = "경로"

Hyphanet을 그냥 사용하면 HDD의 부담이 크기 때문에 메모리가 있다면 TEMP 폴더를 RAMDisk로 바꾸는 것을 추천한다. "경로"에 RAMDisk의 폴더 (예 : Z:TEMP)를 지정하면 TEMP 폴더가이 위치에 만들어 HDD의 부담을 줄일 수 있다. 폴더의 파일은 Hyphanet을 재시작 할 때마다 재설정되기 때문에 PC 종료 시 내용이 지워 RAMDisk도 문제없다.

4.6.3. Hyphanet 본체 설정

브라우저 화면에서 "Configuration → Core Settings"
· Upload bandwidth limit 100KiB 이상
· Download bandwidth limit 100KiB 이상

최대 업, 다운 속도. 대역에 여유가 있으면 1MB 이상도 좋다.
· Hyphanet datastore size 20GB 이상

Hyphanet 캐시 용량. 파일을 다운로드할 때 캐시에 파일이 있으면 그만큼 빨리 완료된다. 외부에서 무엇이 들어올지는 전혀 모르기 때문에 여유가 있으면 가능하면 늘려 두 자.

4.6.4. Frost 설정

· Options → Preferences → News (1) 항목
· 'Number of days to display'와 'Number of days to download backwards'를 30~180

특히 처음 시작하는 경우, 이전 게시물을 검색해야 하므로 큰 값으로 둔다.
· 'Always download all days backward'와 'Silently retry failed message uploads'를 체크한다.

· Minimum update interval of a board: 1 이상
· Number of concurrently updating boards: 6~20

4.7. Hyphanet 삭제법

Windows를 사용하는 경우, 제어판 -> '프로그램 및 기능'[4]에서 Hyphanet을 선택하여 삭제할 수 있다.

5. Hyphanet(Darknet 모드) 사용법

> - Best case: If a local politician would want to find you, after you uploaded proof that he takes bribes, and you uploaded the files to a new safe key (SSK) and used Freenet in Darknet-mode with connections only to friends who would rather die than let someone take over their computer, there's no way in hell, you'd get found due to Freenet (the file data could betray you, or they could find you by other means, but Freenet won't be your weak spot).
> - Don't let others know the data you are going to upload before the upload finished (would allow some attacks).
> - Use only Darknet with trusted friends (Darknet means that you connect only to people you know personally. For that it is necessary to know other people who use Freenet).
> - Upload small files, so the time in which you are actively uploading is short.
> - Use an OS without trojans. So no Windows. (Note: Linux can be hacked, too, but it is far less likely to already have been compromised)
> - 최상의 시나리오: 만약 지역 정치인이 당신을 찾으려고 한다면, 당신이 그가 뇌물을 받았다는 증거를 업로드한 후, 해당 파일을 새로운 안전 키(SSK)에 저장하고 Freenet을 다크넷 모드로 사용하며, 컴퓨터 해킹을 당하느니 차라리 죽는 게 낫다고 생각할 정도로 믿을 수 있는 친구들과만 연결한다면, Freenet 덕분에 발각될 가능성은 거의 없습니다. (파일 데이터 자체에 문제가 있거나 다른 방법으로 발각될 수는 있겠지만, Freenet이 당신의 약점이 되지는 않을 겁니다.)
> - 업로드가 완료되기 전까지는 업로드할 데이터를 다른 사람에게 알리지 마세요. (공격에 취약해질 수 있습니다.)
> - 신뢰할 수 있는 친구들과만 다크넷을 사용하세요. (다크넷은 개인적으로 아는 사람들과만 연결하는 것을 의미합니다. 이를 위해서는 Freenet을 사용하는 다른 사람들을 알아야 합니다.)
> - 업로드하는 데 걸리는 시간을 최소화하기 위해 작은 파일을 업로드하세요.
> - 트로이목마가 없는 운영체제를 사용하세요. 따라서 Windows는 사용하지 마세요. (참고: Linux도 해킹될 수 있지만, 이미 해킹당했을 가능성은 훨씬 낮습니다.)
>
> https://www.draketo.de/light/english/freenet/anonymity-best-case-and-worst-case

https://www.draketo.de/english/freenet/connect-speak-freely

Hyphanet의 Darknet 모드는 Tor의 Directory Authorities, I2P의 Reseed Servers, Hyphanet Opennet 모드의 Seed Nodes같은 통신 과정에서 중앙 집중적인 구간이 없다. 그러므로 검열이 매우 어렵다.

위 글과 아래의 이미지를 참고하여 Hyphanet의 Darknet 모드를 이용할 수 있다.

5.1. 설정하기

http://127.0.0.1:8888/wiz/

Set Up Freenet

If you are using a thirdparty IME (Input Method Editor, used as text input for common asian languages), please disable it for Freenet and use an IME from your Operating System. There have been reports of the IME collecting your keystrokes and sending them to remote servers.
Voice recognition has also been used for on-device surveillance.

Network Security

- [x] I know someone who runs Freenet.
- [ ] I want to connect to untrusted strangers to improve performance.

Bandwidth

- [ ] I have a monthly bandwidth limit.

1024 KiB/s download. 160 KiB/s upload.

Common Internet connection speeds

Connection type	Download limit	Upload limit
Detected	unavailable KiB/s	unavailable KiB/s
4 megabits	256 KiB/s (2 Mbps)	16 KiB/s
VDSL	2048 KiB/s (16 Mbps)	160 KiB/s

Storage

Give 1.00 GiB of storage space to Freenet.

- [ ] I want Freenet to require a password when it starts.

Finish

Protection against a stranger attacking you over the Internet

Do you know personally anyone who already uses Freenet? If you know at least 3 people who already use Freenet, you can enable darknet mode, so Freenet will only connect to your Friends, greatly improving security. However, if you don't know anyone already on Freenet, or if you want maximum performance, you should enable opennet mode, and Freenet will automatically connect to other Freenet nodes run by strangers (as well as your Friends).

Opennet mode (connect to strangers and friends): I don't know anyone who already uses Freenet: Connect to other Freenet nodes automatically.

- ○ **LOW**: I do not care about monitoring and want maximum performance.

It may be quite easy for others to discover your identity!

- ○ **NORMAL**: I live in a relatively free country, but I would like to make it more difficult for others to monitor my communications.

Freenet will be reasonably careful to protect your anonymity, at some performance cost. You should add friends running Freenet and upgrade to HIGH when you are able.

Darknet mode (connect to friends only): I know at least 3 people (10+ for good performance) who already use Freenet: Connect only to Friends.

- ◉ **HIGH**: I would like to make it much more difficult for others to monitor my communications, or I am worried about ISPs and/or governments trying to block Freenet.

Only connecting to Friends massively improves security, but Freenet will be slow unless you add at least 5-10 friends.

- ○ **MAXIMUM**: I intend to access information that could get me arrested, imprisoned, or worse. I understand that Freenet is experimental and cannot ensure security against certain known attacks, but I accept the risks compared to the alternatives.

*Freenet will be **significantly** slower than in HIGH, as well as only connecting to Friends. Your real identity should be relatively safe provided you only connect to people you trust. For a more detailed explanation of Freenet's security, see the bottom of the "who should Freenet connect to?" page of the wizard.*

Freenet - Freenet

http://127.0.0.1:8888

BROWSING FILESHARING FRIENDS DISCUSSION STATUS CONFIGURATION SHARESITE

Security Levels
Plugins
Web interface
Logs
Core settings
Auto-update
Translation

Configure the level of security provided by Freenet

No friends found

Your Freenet node has no friends to connect to, therefore it will not be able to work normally. You need at least 3 co… …ll times, and ideally 5-10. These should be people you know who also run Freenet. Alternatively you could set the network security level to NORMAL or LOW… …ting to strangers and quickly get some connections.

Could not load plugin!

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes … doesn't exist for key CHK@IQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVIUFQAJvUzjs,AAMC--8

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

My bookmarks ***[Edit]***

Starting Points

activelink
Freenet First Steps
(Starting with Freenet)

activelink
Clean Spider
(An automated index with strict filtering)

Index of Indexes
(A collaborative index of indexes)

Freenet related software

http://127.0.0.1:8888/seclevels/ Messages: 1 Warnings English Switch to advanced mode Security levels:HIGH LOW 0

http://127.0.0.1:8888/seclevels/

BROWSING FILESHARING FRIENDS DISCUSSION STATUS CONFIGURATION SHARESITE

Security levels

http://127.0.0.1:8888/wizard/?step=OPENNET

Who should Freenet connect to?

Freenet is designed to prevent your chat messages, downloads, browsing etc from being traced back to you. Freenet can only provide strong protection when you know the people you are directly connected to.

- (●) **Only connect to your friends:**

Advantage: Very hard to trace anything on Freenet back to you.[1]
Disadvantage: You need at least 5 friends that use Freenet.

- ( ) **Connect to strangers:**

Advantage: No need to know anyone that uses Freenet.
Disadvantage: Much easier to trace your messages, files, etc back to you.

Back Next

[1]: Freenet provides reasonable anonymity and is very hard to block, IF: (touch to see)

1. You don't do anything that could reveal your identity, e.g. use your real name, post your home address on a chat board or talk about people you know personally. Other personally identifying information includes common sense stuff like where you went to school but also your IP address, your Freenet port numbers, and in some cases your Freenet logs and statistics. If you have a problem with Freenet you should usually make a new identity before asking for help.
2. You only connect to your friends.[2]
3. Your friends are trustworthy (but strangers are always worse than friends).
4. Possible attackers don't already know or suspect who or where you are: they only know you are a particular identity on Freenet.
5. You change your anonymous identity occasionally (e.g. on forums).
6. You always upload files safely. Freenet will remind you how to do this.
7. Your friends keep their computers secure.
8. You are part of a big network (e.g. the main Freenet which you get if enabling connecting to strangers) or part of a private network which the attackers do not know about.
9. You are not too close to strangers. If for instance your friends connect to strangers, you may not be safe against a very powerful attacker. Most people shouldn't worry too much about this, it will improve as your friends connect their friends and no longer need strangers.
10. There aren't any horrible bugs in Freenet. Every program of reasonable size contains bugs. We hope no serious ones which would affect your anonymity are left in freenet, but we might have missed them. You have been warned!

[2]: For now you probably want to connect to strangers just to get connected. However, a determined attacker may be able to trace your uploads/downloads/chat/etc back to you, so don't do this if you are planning to upload dangerous content. In the long term we hope everyone will connect only to their friends as this is much safer.

Protection against a stranger attacking you over the internet (only connect to friends)

Freenet will only connect to your friends, making it very difficult for anyone to trace your Freenet usage. How concerned are you about people you don't know trying to trace you?

- ( ) **HIGH**: I would like to make it much more difficult for others to monitor my communications, or I am worried about ISPs and/or governments trying to block Freenet.

Only connecting to Friends massively improves security, but Freenet will be slow unless you add at least 5-10 friends.

- (●) **MAXIMUM** I intend to access information that could get me arrested, imprisoned, or worse. I understand that Freenet is experimental and cannot ensure security against certain known attacks, but I accept the risks compared to the alternatives.

*Freenet will be **significantly** slower than in HIGH, as well as only connecting to Friends. Your real identity should be relatively safe provided you only connect to people you trust. For a more detailed explanation of Freenet's security, see the bottom of the "who should Freenet connect to?" page of the wizard.*

Adding people as Friends who you don't know outside of Freenet will not improve security and will reduce performance!

Back Next

Add friends or Freenet cannot connect!

WARNING: You are about to set the maximum network security level! This will **significantly** slow down Freenet for you! Please do not do this unless you really need the security! **You must know at least one person already running Freenet**, preferably 3, 5-10 for good performance. You must add them on the Friends page. These must be people you already know and at least marginally trust.

- [x] Yes I really want to enable maximum security, I understand that Freenet is still experimental and it may still be possible to trace me, and that this setting may dramatically reduce Freenet's performance!

Back Next

Protection of your downloads, uploads and Freenet browsing cache

How concerned are you about people stealing or seizing your computer?

SecurityLevels.physicalThreatLevelTruecrypt On some versions of Windows you can encrypt your swapfile with the command "fsutil behavior set encryptpagingfile 1".

Also, you should encrypt your swap space if possible (this is a temporary file used by Windows to provide extra space if it runs out of memory). This may be easier to set up than full disk encryption.

- ( ) **NONE**: Don't encrypt anything. (Choose only if you are using full disk encryption)
- ( ) **LOW**: Protect the downloads, uploads, and Freenet browsing cache, with a persistent encryption key so they can be wiped quickly.
- ( ) **HIGH**: Protect the downloads, uploads, and Freenet browsing cache with a password.

Set the password: Confirm password:

- (●) **MAXIMUM** Use a temporary encryption key, so that downloads, uploads and Freenet browsing cache are wiped on restarting Freenet.

You should follow standard security precautions (keep updated, run an anti-virus, don't open files you don't trust etc), and note that if they capture your computer while it is switched on and running Freenet, no amount of encryption will help you!

Back Next

Node name required!

Please enter a node name in the field below (we recommend a nickname possibly with an email address). This is so that your friends (trusted peers, which you have manually added) can easily tell your node from their other nodes. This is not visible to strangers (untrusted automatically added peers). Note that any friend or stranger may trivially identify you from your IP address, since you are connected to them, but they cannot easily tell what you are requesting.

test123

Back Next

Datastore size

Please select a size for your datastore. Recommended values lie between 1GiB and 20GiB. A smaller datastore can result in problems downloading files, a larger datastore is beneficial to the network but might slow down your computer due to high filesystem load, especially in the first few hours after installation. The datastore acts like a cache; storing data for the network will help you to get better throughput when requesting popular files. The more space you can afford the better it is for the community and the faster your node and especially your downloads will go.

Current size: 1.0 GiB

Back Next

Bandwidth Limits

Does your internet connection have a monthly data limit?

Yes No

Back

Transfer Rate Limit

How fast is your Internet connection? Freenet should use no more than half of it. You can change this setting later on the **Core settings** page. Note that 1 megabit per second (1 Mbps) = 125 kilobytes per second (125 KB/s).

Connection type	Download limit	Upload limit	Select
Current bandwidth limit	1.0 MiB/s (= 8Mbps)	160 KiB/s	(●)
6 megabits (average ADSL1)	384 KiB/s (= 3Mbps)	16.0 KiB/s	( )
8 megabits (fast ADSL1)	512 KiB/s (= 4Mbps)	32.0 KiB/s	( )
12 megabits (slow ADSL2)	768 KiB/s (= 6Mbps)	64.0 KiB/s	( )
Fast DSL (160KiB/s up)	768 KiB/s (= 6Mbps)	160 KiB/s	( )
VDSL (20/5)	1.25 MiB/s (= 10Mbps)	320 KiB/s	( )
100 megabits (fibre)	2.0 MiB/s (= 16Mbps)	2.0 MiB/s	( )

Enter a custom bandwidth limit

Back Next

5.2. 친구와 서로 연결하기

Freenet - Freenet

http://127.0.0.1:8888

BROWSING FILESHARING FRIENDS DISCUSSION STATUS CONFIGURATION SHARESITE

Connections to friends

Add a Friend

Connect to a friend running Freenet to improve your security

s found

Your Freenet node has no friends to connect to, therefore it will r… …at all times, and ideally 5-10. These should be people you know who also run Freenet. Alternatively you could set the network security level to NORMAL or LOW to enable connecting to strangers and quickly get some connections.

Could not load plugin!

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes to be sure the data doesn't exist for key CHK@lQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVlUFQAJvUzjs,AAMC--8/KeyUtils.jar

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

My bookmarks *[Edit]*

Starting Points

Freenet First Steps
(Starting with Freenet)

Clean Spider
(An automated index with strict filtering)

Index of Indexes
(A collaborative index of indexes)

Freenet related software

http://127.0.0.1:8888/addfriend/ Messages: 1 Warnings English Switch to advanced mode Security levels: MAXIMUM MAXIMUM 0

Why you should connect to your friends running Freenet

You can improve Freenet's security by connecting to your friends. That is, to people you actually know who also run Freenet. These can be online acquaintances, but do not add connections to total strangers, as adding strangers as Friends will not improve security much and will cause problems for the network as a whole if lots of people do it. When you have added enough Friends, so that at least 5 are online at all times, you can increase your network security level to HIGH, and only connect to Friends, which is called "darknet mode". This makes it much harder for an attacker to even find out that you are running Freenet, and makes most attacks against your anonymity much harder. Freenet will make encrypted connections to your friends directly over the Internet, so only add people you can already be easily connected to (family, coworkers, real life friends, online friends).

In order to connect to a Friend, you need to exchange noderefs with them. A noderef is a small file which contains the information needed for their copy of Freenet ("Freenet node") to connect to yours. You must add their noderef and they must add your noderef, for the two nodes to connect. See below for your noderef.

Freenet has not yet managed to download the Windows installer, however you can get it over Freenet here.

Freenet has not yet managed to download the non-Windows installer, however you can get it over Freenet here. This is a jar file which must be opened with java; hopefully your friend can double click on it, but if that doesn't work try opening a command line and typing "java -jar freenet-latest-installer-nonwindows.jar".

Connect to a Friend

Enter node reference directly:

OR enter the URL or KEY of the node reference here:

OR browse for the node reference file here: 찾아보기... 선택된 파일 없음

How much do you trust this friend? A higher trust level will improve performance for you and your friend. But this makes you more vulnerable if they are untrustworthy, or their computer is hacked or seized.

- **HIGH**: I trust my friend, and I trust his ability to secure his computer. Share as much information as possible to maximise performance.
- **NORMAL**: I trust my friend a little. Share some information, but take some precautions. Moderate performance gain.
- **LOW**: I don't trust my friend. Share as little as possible. Lower performance. Note that this is still safer than connecting to strangers in almost all cases.

Do you want your other friends to be able to see and connect to this friend? If you let your friends see this friend, and this friend see your friends, it will improve performance significantly. However you might not want your other friends to know about this one (but bear in mind that anyone who can see your internet connection might be able to link you). They can also disable being seen by your friends.

- **YES**: Tell my other friends about this friend, and tell this friend about my other friends. They will be able to connect immediately even if I am offline, improving performance significantly.
- **NAME ONLY**: Tell this friend our other friends' nicknames, and tell our other friends this friend's nickname, so they can connect if they know each other.
- **NO**: Don't tell my friends about this friend, and don't let them tell their other friends about me: they are a secret contact.

Enter description:

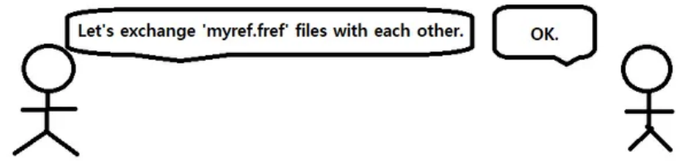
Add

My Node Reference (as text)

다운로드 > 로컬 디스크 (C:) > 사용자 > Administrator > 다운로드

새로 만들기 정렬 보기

myref.fref



Connect to a Friend

Enter node reference directly:

OR enter the URL or KEY of the node reference here:

OR browse for the node reference file here: 찾아보기... myref.fref

How much do you trust this friend? A higher trust level will improve performance for you and your friend. But this makes you more vulnerable if they are untrustworthy, or their computer is hacked or seized.

- **HIGH**: I trust my friend, and I trust his ability to secure his computer. Share as much information as possible to maximise performance.
- **NORMAL**: I trust my friend a little. Share some information, but take some precautions. Moderate performance gain.
- **LOW**: I don't trust my friend. Share as little as possible. Lower performance. Note that this is still safer than connecting to strangers in almost all cases.

Do you want your other friends to be able to see and connect to this friend? If you let your friends see this friend, and this friend see your friends, it will improve performance significantly. However you might not want your other friends to know about this one (but bear in mind that anyone who can see your internet connection might be able to link you). They can also disable being seen by your friends.

- **YES**: Tell my other friends about this friend, and tell this friend about my other friends. They will be able to connect immediately even if I am offline, improving performance significantly.
- **NAME ONLY**: Tell this friend our other friends' nicknames, and tell our other friends this friend's nickname, so they can connect if they know each other.
- **NO**: Don't tell my friends about this friend, and don't let them tell their other friends about me: they are a secret contact.

Enter description:

Add

Added some Friends

Name of result **Number of results**

Added successfully 1

Add another Friend

Go to the Friends page to see whether this friend connects

Return to your Freenet homepage

http://127.0.0.1:8888/friends/

BROWSING FILESHARING FRIENDS DISCUSSION STATUS CONFIGURATION SHARESITE

Only 1 open connection(s)

This node only has one connection. Performance will be impaired, and you have no anonymity nor even plausible deniability if that one person is malicious. Your node is

attached to the network like a "leaf" and does not contribute to the network's health. Try to get at least 3 (ideally more like 5-10) connected peers at any given time.

Could not load plugin!

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes to be sure the data doesn't exist for key CHK@lQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVIUFQAJvUzjs,AAMC--8/KeyUtils.jar

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

My Friends (trusted peers added by me)

Nickname for this node: test123 [Change]

	Status	Name	Trust level	Visible to friends?	Address	Version	Connected / Idle	Private Note
☐	CONNECTED	test456	LOW	NO	[redacted]	1503	3s	

Send confidential message

-- Select action -- Go

Change trust to HIGH

Change visibility to YES

Messages: 1 Warnings English Switch to advanced mode Security levels:MAXIMUM MAXIMUM 1 / 1

5.3. 메시지(N2NTM) 보내기

Hyphanet의 Darknet 모드에는 N2NTM(Node to Node Text Message)이라는 메시지 기능이 있다.

My Friends (trusted peers added by me)

Nickname for this node: test123 [Change]

	Status	Name	Trust level	Visible to friends?	Address	Version	Connected / Idle	Private Note
☐	CONNECTED	test456	LOW	NO	[redacted]	1503	3s	

Send confidential message

-- Select action -- Go

Change trust to HIGH

Change visibility to YES

Messages: 1 Warnings English Switch to advanced mode Security levels:MAXIMUM MAXIMUM 1 / 1

Send Node to Node Text Message

Composing N2NTM to send to the following peers:

- test456

test1

Send message

Peer Name	N2NTM Send Status
test456	Sent
test1	

Return to your Freenet homepage

- Friends

BROWSING FILESHARING FRIENDS DISCUSSION STATUS CONFIGURATION SHARESITE

Messages — Detailed status alerts and messages from your Friends

Statistics

Diagnostic

Internet connection

Only 1 open connectio

This node only has one connection. Performance will be impaired, and you have no anonymity nor ev … if that one person is malicious. Your node is attached to the network like a "leaf" and does not contribute to the network's health. Try to get at leas … 10) connected peers at any given time.

Could not load plugi

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes to be sure the data doesn't exist for key CHK@lQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVIUFQAJvUzjs,AAMC--8/KeyUtils.jar

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

Node to Node Text Message 1 from test123 ([redacted])

From: test123 (26. 2. 1 오후 8:50)

test1

Reply

Delete

Messages: 1 Warnings, 1 Minor English Switch to advanced mode Security levels:MAXIMUM MAXIMUM 1 / 1

5.4. 파일 공유하기

BROWSING | FILESHARING | FRIENDS | DISCUSSION | STATUS | CONFIGURATION | SHARESITE

Downloads
Uploads
Upload a file
Upload a file to Freenet

Only 1 open connection(s)

This node only has one connection. Perfor paired, and you have no anonymity nor even plausible deniability if that one person is malicious. Your node is attached to the network like a "leaf" and do to the network's health. Try to get at least 3 (ideally more like 5-10) connected peers at any given time.

Could not load plugin!

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes to be sure the data doesn't exist for key CHK@lQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVlUFQAJvUzjs,AAMC--8/KeyUtils.jar

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

Upload a file to Freenet

There are several different ways to upload (insert) a file to Freenet depending on whether you have uploaded the file before and what your security requirements are:

- **Insert a canonical key**: This will always produce the same key for the same file, so is convenient for filesharing. However, if the bad guys can predict what files you are going to insert, they may be able to use this to trace you a lot more easily.
- **Insert a random, safe key** This is much safer than the first option, but the key will be different every time you or somebody else inserts the key. Use this if you are the original source of some sensitive data.

Upload a file from disk: Browse files...

Or upload a file through the browser (SLOW): 찾아보기... 선택된 파일 없음 Insert File

Directory Listing: C:\Users\Administrator\Desktop

	File	Size
	B:\	
	C:\	
	Y:\	
	..	
Insert	새 폴더	
Insert	[redacted]	382 KiB
Insert	[redacted]	908 B
Insert	test1.txt	19 B

Completed uploads (1)

Remove from list | Remove all finished uploads

Recommend files to friends

	Local path	Size	Key
☑	C:\Users\Administrator\Desktop\test1.txt	19 B	SSK@.../test1.txt

Remove from list | Remove all finished uploads

Recommend files to friends

Messages: 1 Warnings, 1 Minor | English | Switch to advanced mode | Security levels: MAXIMUM MAXIMUM | 1 / 1

Recommend a file to friends

Key:
freenet:SSK@PpS9eHmwbP6zd0aGrQecZJGjR~PCtzyLxHkzuFYP9Xw,0CJ7P0TjJJpNjnU7PA9H8BFc0HN1CiKp~la~FokPU6Q,AQACAAE/test1.txt
Description of the file:

☐ **Recommend to friends**

☑ test456

Recommend

BROWSING | FILESHARING | FRIENDS | DISCUSSION | STATUS | CONFIGURATION | SHARESITE

Messages
Statistics
Diagnostic
Internet connection
Detailed status alerts and messages from your Friends

Only 1 open connection(s)

This node only has one connection. Performance will be impaired, and you have no anonymity nor even plausible deniability if that one person is malicious. Your node is attached to the network like a "leaf" and does not contribute to the network's health. Try to get at least 3 (ideally more like 5-10) connected peers at any given time.

Could not load plugin!

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes to be sure the data doesn't exist for key CHK@lQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVlUFQAJvUzjs,AAMC--8/KeyUtils.jar

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

Node to Node Text Message 1 from test123 ([redacted])

From: test123 (26. 2. 1 오후 8:50)

test1

Reply

Delete

test123 recommends you a file

SSK@.../test1.txt

Delete

Messages: 1 Warnings, 2 Minor | English | Switch to advanced mode | Security levels: MAXIMUM MAXIMUM | 1 / 1

BROWSING | FILESHARING | FRIENDS | DISCUSSION | STATUS | CONFIGURATION | SHARESITE

Downloads
Uploads
Upload a file
Files being downloaded from Freenet

connection(s)

This node only has one connection. Perfor paired, and you have no anonymity nor even plausible deniability if that one person is malicious. Your node is attached to the network like a "leaf" and do to the network's health. Try to get at least 3 (ideally more like 5-10) connected peers at any given time.

Could not load plugin!

The plugin KeyUtils could not be loaded: error while fetching plugin: Route not found - could not find enough nodes to be sure the data doesn't exist for key CHK@lQs-ssTnVh8ZuvYASea-O78hVA2y81FI7AVf2X5PXJI,J7yf0iM5Q1W4MppL0DITyeKJMDdVQQiVlUFQAJvUzjs,AAMC--8/KeyUtils.jar

We are still trying to load the plugin over Freenet.

You can try again.

Don't try again on next startup

Bulk downloads

You can paste a list of keys to download in the box below (one per line)

SSK@PpS9eHmwbP6zd0aGrQecZJGjR~PCtzyLxHkzuFYP9Xw,0CJ7P0TjJJpNjnU7PA9H8BFc0HN1CiKp~la~FokPU6Q,AQACAAE/test1.txt

Filter: ☑ Select this to run your request through the content filter. The filter will try to prevent your computer from running anything which might harm it, or break your anonymity. Keeping this checked is strongly recommended.

Download

Bulk downloads

The following 1 keys have been enqueued sucessfully:
- freenet:SSK@PpS9eHmwbP6zd0aGrQecZJGjR~PCtzyLxHkzuFYP9Xw,0CJ7P0TjJJpNjnU7PA9H8BFc0HN1CiKp~la~FokPU6Q,AQACAAE/test1.txt

Return to queue page

Completed fetches to temporary space (1)

6. Hyphanet을 권장하지 않는 이유

> The appropriateness for use in hostile regimes against state level adversaries has been **tremendously overstated**.
> 국가 수준의 적대 세력에 대항하기 위한 용도에 대한 적절성은 **엄청나게 과장되었다**.
>
> https://geti2p.net/en/docs/how/tech-intro @

> It does not provide strong anonymity, rather it relies on **plausible deniability**.
> 그것은 강력한 익명성을 제공하지 않고 오히려 **그럴듯한 부인 가능성**에 의존합니다.
>
> https://www.reddit.com/r/darknet/comments/10uf8rw/why_freenet_project_is_never_discussed_here/ @

> Freenet uses a complexly random routing process to make it hard (arguably impossible) for adversaries to distinguish "active" nodes (those that upload stuff, those that store stuff, and those that download stuff) from "passive" nodes, which merely relay stuff to other nodes.
> Freenet is designed to provide **plausible deniability**, whereas Tor is designed to provide anonymity for clients and .onion servers.
> Freenet은 복잡하고 무작위적인 라우팅 프로세스를 사용하여 적대 세력이 "활성" 노드(파일을 업로드하는 노드, 파일을 저장하는 노드, 파일을 다운로드하는 노드)와 "수동" 노드(단순히 다른 노드로 파일을 전달하기만 할 뿐인 노드)를 구별하기 어렵게(아마도 불가능할 수도 있음) 만듭니다.
> Freenet은 **그럴듯한 부인 가능성**을 제공하도록 설계된 반면, Tor는 클라이언트와 .onion 서버에 익명성을 제공하도록 설계되었습니다.
>
> https://www.reddit.com/r/Freenet/comments/a0cwx3/deleted_by_user/ @

> **Freenet was never anonymous really**, freenet was meant to provide **deniability and censorship resistance**; that is different.
> Anonymity is lack of identification whereas censorship-resistance is availability of information. Freenet's model is about preventing denial of access to information via a distributed datastore couple with reasonably deniable attribution of specific action.
> **프리넷은 실제로 익명이 아니었습니다**. 프리넷은 **부인 가능성과 검열 저항성**을 제공하기 위해 만들어졌지만, 그것은 다릅니다.
> 익명성은 식별의 부족인 반면 검열 저항성은 정보의 가용성입니다. Freenet의 모델은 특정 행동에 대한 합리적으로 부인 가능한 귀속과 함께 분산 데이터 저장소를 통한 정보 접근 거부를 방지하는 것입니다.
>
> https://www.reddit.com/r/Freenet/comments/7a00fj/would_routing_through_i2p_solve_all_of_freenets/ @

> I'm not saying Freenet here is 100% broke but it's primary purpose/use is post-distribution **censorship resistance**. **If you want anonymity go with another solution**. I'm also not knocking Freenet here nor it's casual anonymity but the fact is there have been several non-trivial attacks and known weakness that have came up in the past decade and there simply is no want to fix them as they all are handwaivum with "use darknet" coupled with "if you use darknet and your peers are compromised, too bad".
> 저는 여기의 Freenet이 100% 망가졌다고 말하는 것이 아니라, 주된 목적/용도는 배포 후 **검열 저항**입니다. **익명성을 원하시면 다른 솔루션을 사용하세요**. 저는 또한 여기의 Freenet이나 캐주얼 익명성을 비난하는 것이 아니지만, 사실 지난 10년 동안 여러 가지 사소하지 않은 공격과 알려진 취약점이 발생했으며, 그것들은 모두 "다크넷을 사용하세요"와 "다크넷을 사용했는데 동료들이 침해당했다면, 안타까운 일"이라는 두 가지가 합쳐진 손쉬운 포기이기 때문에 그것들을 고칠 필요가 없습니다.
>
> https://www.reddit.com/r/Freenet/comments/7a00fj/would_routing_through_i2p_solve_all_of_freenets/ @

Hyphanet에 대해 조사해 보면 Hyphanet이 생각보다 더 안전하지 않다는 사실을 알게 된다. 양자컴퓨터와 AI가 발달하면서 기존에는 어려웠던 고난이도의 연산이 가능해지고 이는 난독화(Obfuscation)[5]를 통한 그럴듯한 거부가능성(plausible deniability)으로 신원을 숨김이 한계에 다다르었음을 의미한다. 처음에는 강력한 검열 저항성(콘텐츠가 삭제되지 않고 계속 살아남음)에 매력을 느끼지만 나중에는 Tor나 I2P에 비해서 부실한 익명성(신원을 식별할 수 없음)이 눈에 거슬리게 된다.

Hyphanet 대신 강력한 익명성을 가지고 있는 Tor나 I2P를 권장한다.

7. Freenet over I2P

> Freenet needs to run on top of a mixnet such as I2P or Tor.
> Freenet은 I2P나 Tor와 같은 믹스넷 위에서 실행되어야 합니다.
>
> https://geti2p.net/en/docs/how/tech-intro @

> Freenet is typically run in “opennet” mode where it connects first to some seed nodes, then to several random strangers (your peers.) This is the most common way to run Freenet as most people don’t already know others they can connect to, so they just let Freenet choose their peers from the available pool of other users. This presents some security risks: if one of those random peers happens to be an adversarial node they now have your IP address, and if more than one are adversarial they could perform what’s known as a “surround attack” and possibly find out what you’re doing on Freenet, breaking both your anonymity and privacy. In any event, total strangers can easily see that you’re using Freenet and you’d probably feel more comfortable if they couldn’t.
> The recommended solution is to run Freenet in “darknet” mode instead, where rather than connecting to random strangers you form a local, friends-and-family, “small world” network composed of people you actually know and trust, with whom you exchange node references, and then only connect to each other rather than to the seed nodes and to random peers. While doing so greatly increases your security, the difficulty is in forming this network in the first place.
> It is recommended that for best performance and anonymity such a network have at least 10 members. How many of us personally know 10 people who 1) we can trust enough to let them know we use Freenet, 2) have both the computer know-how and the interest to want to do likewise, 3) can be relied on to follow best practices regarding security and anonymity, and 4) are likely to leave their computer and Freenet running 24x7? Not very many of us unless we happen to have a large circle of family and friends who are mostly computer geeks and privacy advocates. We would be lucky if we knew one or two such real-life friends.
> This freesite offers a possible solution.

> FYI, I2P was preferred over TOR as the anonymous network of choice to due to the fact that an increase in overa ll traffic and number of users on I2P increases its network routing efficiency as well as everyone's anonymity, so they welcome users who use I2P for higher-traffic activities such as bit torrenting for example, while TOR discour ages these activities on their network as such things would consume too many of its resources and could cause problems for other users. It comes down to how I2P's "garlic routing" works vs. TOR's "onion routing."
> Freenet은 일반적으로 "opennet" 모드로 실행되며, 먼저 일부 시드 노드에 연결한 다음 여러 무작위 낯선 사람(귀하의 피어)에 연결합니다. 이것은 Freenet을 실행하는 가장 일반적인 방법입니다. 대부분의 사람들은 연결할 수 있는 다른 사람을 이미 알지 못하기 때문에 Freenet이 다른 사용자의 사용 가능한 풀에서 피어를 선택하도록 합니다. 여기에는 몇 가지 보안 위험이 있습니다. 이러한 무작위 피어 중 하나가 적대적 노드인 경우 이제 귀하의 IP 주소를 가지고 있고, 두 명 이상이 적대적이면 "서라운드 공격"이라고 알려진 것을 수행하여 귀하가 Freenet에서 무엇을 하는지 알아낼 수 있으며, 귀하의 익명성과 프라이버시가 모두 깨집니다. 어떤 경우든 완전히 낯선 사람은 귀하가 Freenet을 사용하고 있다는 것을 쉽게 알 수 있으며, 그들이 알 수 없다면 귀하는 더 편안할 것입니다.
> 권장되는 해결책은 대신 "darknet" 모드에서 Freenet을 실행하는 것입니다. 여기서는 무작위 낯선 사람에게 연결하는 대신 실제로 알고 신뢰하는 사람들로 구성된 로컬, 친구 및 가족, "작은 세상" 네트워크를 형성하고, 노드 참조를 교환한 다음 시드 노드 및 무작위 피어가 아닌 서로에게만 연결합니다. 이렇게 하면 보안이 크게 향상되지만, 어려움은 처음에 이 네트워크를 형성하는 것입니다.
> 최상의 성능과 익명성을 위해 이러한 네트워크에는 최소 10명의 멤버가 있는 것이 좋습니다. 우리 중 얼마나 많은 사람이 1) Freenet을 사용한다는 것을 알릴 만큼 신뢰할 수 있고, 2) 컴퓨터 노하우와 마찬가지로 하려는 관심이 있고, 3) 보안 및 익명성과 관련된 모범 사례를 따를 것으로 신뢰할 수 있고, 4) 컴퓨터와 Freenet을 24시간 내내 실행할 가능성이 있는 10명을 개인적으로 알고 있습니까? 컴퓨터 괴짜이자 개인 정보 보호 옹호자인 가족과 친구로 구성된 큰 서클이 있지 않는 한 우리 중 많은 사람이 그렇지 않습니다. 우리는 그런 실제 친구 한두 명을 안다면 운이 좋았을 것입니다.
> 이 프리사이트는 가능한 해결책을 제공합니다.
> FYI, I2P는 전체 트래픽과 I2P의 사용자 수가 증가함에 따라 네트워크 라우팅 효율성과 모든 사람의 익명성이 증가하기 때문에 TOR보다 익명 네트워크로 선호되었습니다. 따라서 비트 토렌팅과 같이 트래픽이 많은 활동에 I2P를 사용하는 사용자를 환영하지만 TOR는 네트워크에서 이러한 활동을 권장하지 않습니다. 이러한 활동은 리소스를 너무 많이 소모하고 다른 사용자에게 문제를 일으킬 수 있기 때문입니다. 결국 I2P의 "마늘 라우팅"과 TOR의 "양파 라우팅"이 어떻게 작동하는지에 달려 있습니다.
>
> https://github.com/eyedeekay/docs-from-freenet/blob/master/freenet-over-i2p.md @

https://github.com/eyedeekay/docs-from-freenet @
https://github.com/eyedeekay/docs-from-freenet/blob/master/freenet-over-i2p.md @

Hyphanet(구 Freenet)과 I2P를 결합하여 Hyphanet의 한계를 극복하고자 했던 시도가 있었다.
해당 freesite에 접속해서 확인해 본 결과, 2024년 기준 웹사이트의 업데이트가 끊겼다.
FMSArchive를 확인해 본 결과, 2024년 기준 'Hyphanet과 I2P의 결합'에 대한 주제는 Hyphanet 이용자들에게 관심을 받지 못하고 있는 것으로 보인다.

8. 억압적인 국가에서의 검열 우회

이 문단의 내용 중 전체 또는 일부는 I2P 문서의 r158 판, 10번 문단에서 가져왔습니다. 이전 역사 보러 가기

> If I take your question as "What to do if I'm worried about getting caught running an I2P router in an oppressive regime," and you are worried about the authorities associating your computers with I2P traffic in the long term, and you still want to run an I2P router, then there are generally two solutions:
>
> - Run I2P off-site somewhere it is legal, and access it via an innocuous-seeming form of encrypted connection, such as an SSH connection or an HTTPS connection.
> - Encapsulate your I2P traffic in something legal. If a VPN is legal, then that I guess. If SSH is legal, an SSH tun nel.
>
> But, suppose your adversary is waiting for you to download a particular file that they know you are going to try and download anonymously. If they observe you downloading something that looks like a file of a similar size o n your HTTPS tunnel or SSH tunnel or VPN, they're just going to assume that file is what they wanted to catch y ou with and come after you anyway.
> In fact, at the point where your adversary is willing to go after all I2P users, or all Tor users, or all bittorrent users or TLS users or bitcoin users or whatever, it's impossible to just give people "Settings" that can guarantee they w ill never be under suspicion. I mean, presumably you got an executable installer from https://i2p.net/, right? S o you made DNS requests that say "I'm interested in I2P" you connected to the I2P web site and you downloade d a file about ~18.5 Mb in size. In such a draconian regime, you either get I2P from an unofficial channel, likely a sneakernet channel, or you are already under suspicion. Then you have to re-seed from a channel that can't be monitored easily as well, hopefully your sneakernet guy brought you a fresh reseed file to start with. You get the internet you use it on with a cantenna. You get the idea. In these kinds of very oppressive regimes, technology must be combined with planning, including possibly escape plans.
> Fortunately, only a few countries have this kind of law so far.
> 만약 당신의 질문을 "억압적인 정권 아래에서 I2P 라우터를 운영하다가 적발될까 봐 걱정된다면 어떻게 해야 할까요?"로 이해한다면, 그리고 당국이 당신의 컴퓨터를 I2P 트래픽과 장기적으로 연관시킬까 봐 걱정되지만, 그럼에도 불구하고 I2P 라우터를 운영하고 싶다면 일반적으로 두 가지 해결책이 있습니다.
>
> - I2P를 합법적인 외부 장소에서 운영하고, SSH 연결이나 HTTPS 연결처럼 무해해 보이는 암호화된 연결을 통해 접속하는 것입니다.
> - I2P 트래픽을 합법적인 방식으로 캡슐화하는 것입니다. VPN이 합법적이라면 VPN을 사용할 수 있고, SSH가 합법적이라면 SSH 터널을 사용할 수 있습니다.
>
> 하지만, 만약 당신의 적이 당신이 익명으로 다운로드하려는 특정 파일을 기다리고 있다고 가정해 봅시다. 만약 적이 당신이 HTTPS 터널이나 SSH 터널, 또는 VPN을 통해 비슷한 크기의 파일을 다운로드하는 것을 목격한다면, 그들은 그 파일이 당신이 익명으로 다운로드하려던 파일이라고 단정짓고 당신을 추적할 것입니다.
> 사실, 적이 모든 I2P 사용자, 모든 Tor 사용자, 모든 Bittorrent 사용자, TLS 사용자, 모든 Bitcoin 사용자 등을 표적으로 삼으려 한다면, 사람들이 절대 의심받지 않도록 보장하는 "설정"을 제공하는 것은 불가능합니다. 예를 들어, 여러분은 https://i2p.net/에서 실행 가능한 설치 프로그램을 다운로드했을 겁니다. 즉, "I2P에 관심이 있습니다"라는 DNS 요청을 보내고, I2P 웹사이트에 접속해서 약 18.5MB 크기의 파일을 다운로드했을 겁니다. 이렇게 엄격한 규제 체제에서는 비공식 채널, 아마도 Sneakernet 채널을 통해 I2P를 다운로드하거나, 아니면 이미 의심을 받는 상황에 놓이게 됩니다. 게다가 감시가 어려운 채널에서 시드 파일을 다시 제공해야 하는데, Sneakernet에서 제공한 파일이 처음부터 새것이기를 바라야겠죠. 인터넷 연결은 안테나 같은 걸로 합니다. 대충 어떤 상황인지 아시겠죠? 이처럼 억압적인 체제에서는 기술과 함께 탈출 계획을 포함한 철저한 준비가 필수적입니다.
> 다행히 현재까지 이러한 법을 제정한 나라는 극소수에 불과합니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

> To me, the safest way to run freenet in a hostile country is the following:
>
> - Know Freenet users either in countries with more relaxed laws or people who know people
> - Install freenet in a VM that's using full disk encryption OR on a VPS in another country. If remote node, conn ect to fproxy via SSH tunnel. Deleting a VM using full disk encryption takes seconds and is hard to recover v aluable data from.
> - Connect with friends as darknet peers. Make sure they're not an informant. This is an opsec thing.
> - Use Freenet

> Never run your node in anything but high security, even once.
> 제 생각에 적대적인 국가에서 Freenet을 안전하게 운영하는 가장 좋은 방법은 다음과 같습니다.
>
> - 법이 비교적 완화된 국가의 Freenet 사용자 또는 그들을 아는 사람들을 통해 Freenet 사용자를 확보하세요.
> - 전체 디스크 암호화를 사용하는 가상 머신(VM) 또는 다른 국가의 VPS에 Freenet을 설치하세요. 원격 노드인 경우 SSH 터널을 통해 fproxy에 연결하세요. 전체 디스크 암호화(Full Disk Encryption)를 사용하는 VM은 삭제하는 데 몇 초밖에 걸리지 않으며 중요한 데이터를 복구하기 어렵습니다.
> - 친구들과 Darknet 피어로 연결하세요. 정보원이 아닌지 반드시 확인하세요. 이는 작전 보안과 관련된 사항입니다.
> - Freenet을 사용하세요.
>
> 노드를 실행할 때는 절대로 최고 수준의 보안 설정 외에는 다른 설정을 사용하지 마십시오. 단 한 번이라도 사용해서는 안 됩니다.
>
> https://www.reddit.com/r/Freenet/comments/bfh6oe/if_you_live_in_very_hostile_region_of_the_world/ @

> If you're going to be in a place where you're worried about that, your laptop will be searched on arrival, and fairly well. You will need to go further, and hide the application. Maybe even compile it once you arrive.
> Being caught with these things on your computer upon entrance to said country might land you in prison.
> 만약 그런 문제가 걱정되는 곳에 가신다면, 도착 시 노트북 검사를 꽤 꼼꼼하게 받게 될 겁니다. 더 나아가, 해당 애플리케이션을 숨겨야 할 수도 있습니다. 어쩌면 도착 후에 직접 컴파일해야 할지도 모릅니다.
> 해당 국가 입국 시 컴퓨터에 이런 것들이 있는 것이 적발되면 투옥될 수도 있습니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

https://www.whonix.org/wiki/Bridges

USER -(SSH)-> VPS -(Tor,I2P,Hyphanet,GNUnet)-> Website

신뢰할 수 있는 VPS에 Tor, I2P, **Hyphanet**, GNUnet 같은 프로그램을 설치하고 SSH로 터널링(Tunnelling)하여 ISP로부터 익명 네트워크 사용을 숨길 수 있다. ISP는 유저가 VPS와 SSH로 통신하고 있다는 사실만 알 수 있다. 단 이용하는 VPS를 신뢰해야 한다는 단점이 있다.

9. 같이 보기

- Tor
- 인터넷 프라이버시

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.